Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Удмуртский государственный университет»
Институт права, социального управления и безопасности
Кафедра информационной безопасности в управлении

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЭЛЕКТРОЭНЕРГЕТИКЕ: СОВРЕМЕННОСТЬ И ПЕРСПЕКТИВЫ

Сборник статей
II Всероссийской студенческой научно-практической конференции
23 апреля 2026 г.

Ижевск
2026

ISBN 978-5-4312-1368-7
DOI 10.35634/978-5-4312-1368-7-2026-1-95

УДК 004:621.31(063)
ББК 16.84я431 + 31.2-057я431
О-136

Рекомендовано к изданию Редакционно-издательским советом УдГУ

Рецензенты: канд. техн. наук, доцент, доцент каф. теплоэнергетики ФГБОУ ВО «Удмуртский государственный университет» **Е. М. Борисова**;
канд. физ.-мат. наук, доцент каф. математического моделирования и информационной безопасности Нефтекамского филиала ФГБОУ ВО «Уфимский университет науки и технологий» **А. Р. Аюпова**.

Научные редакторы: Т. Н. Стерхова, канд. техн. наук, доцент, доцент каф. информационной безопасности в управлении ИПСУБ ФГБОУ ВО «Удмуртский государственный университет»;
Ф. А. Абашева, канд. юрид. наук, доцент, доцент каф. уголовного процесса и криминалистики ИПСУБ ФГБОУ ВО «Удмуртский государственный университет».

О-136 Обеспечение информационной безопасности в электроэнергетике: современность и перспективы : сб. ст. II Всерос. студ. науч.-практ. конф. / науч. ред. Т. Н. Стерхова, Ф. А. Абашева. – Ижевск : Удмуртский университет, 2026. – 1 DVD-R (3 Мб). – Текст : электронный.

Сборник содержит статьи студентов – участников Всероссийской научно-практической конференции «Обеспечение информационной безопасности в электроэнергетике: современность и перспективы», проведенной Институтом права, социального управления и безопасности Удмуртского государственного Университета 23 апреля 2026 года. В статьях рассматриваются актуальные вопросы обеспечения информационной безопасности в электроэнергетике.

Минимальные системные требования:
Celeron 1600 Mhz; 128 Мб RAM; Windows XP/7/8 и выше, 8x DVD-ROM
разрешение экрана 1024×768 или выше; программа для просмотра pdf.

ISBN 978-5-4312-1368-7

DOI 10.35634/978-5-4312-1368-7-2026-1-95

Обеспечение информационной безопасности в электроэнергетике: современность и перспективы
Сборник статей II Всероссийской студенческой научно-практической конференции
23 апреля 2026 г.

Подписано к использованию 11.08.2026
Объем электронного издания 3 Мб, тираж 10 экз.
Издательский центр «Удмуртский университет»
426034, г. Ижевск, ул. Ломоносова, д. 4Б, каб. 021
Тел.: +7(3412)263-751 E-mail: editorial@udsu.ru

УДК 621.382.3(045)

М. Ф. Абдуллин, С. А. Лесников,
обучающиеся 2 курса Института права,
социального управления и безопасности ФГБОУ ВО «УдГУ».
Научный руководитель: Т. Н. Стерхова, канд. техн. наук, доцент
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Исследование усилителя переменного напряжения на биполярных транзисторах

В работе проведено исследование усилительного каскада переменного напряжения, выполненного по схеме с общим эмиттером на биполярном транзисторе 2N2219. Моделирование осуществлялось в программной среде Micro-Cap в режиме анализа переходных процессов. Определена рабочая точка каскада по постоянному току, измерены параметры входного и выходного сигналов, вычислен коэффициент усиления по напряжению. Получено значение Ku = 189. Продемонстрировано влияние шага дискретизации на форму выходной осциллограммы. Подтверждён инвертирующий характер каскада.

Усилители переменного напряжения на биполярных транзисторах являются фундаментальным классом аналоговых электронных устройств. Схема с общим эмиттером обеспечивает наибольший коэффициент усиления по напряжению среди трёх базовых схем включения транзистора и широко применяется в предварительных каскадах усилителей звуковой частоты, измерительной аппаратуре и радиоприёмных устройствах. Целью работы является исследование характеристик усилительного каскада на транзисторе 2N2219 методом схемотехнического моделирования в среде Micro-Cap, определение коэффициента усиления по напряжению и анализ влияния параметров численного расчёта на отображение результатов.

Биполярный транзистор представляет собой полупроводниковый прибор, состоящий из трех областей с чередующимися типами электропроводности, пригодный для усиления мощности[1]. Принципиальная схема исследуемого усилителя представлена на рисунке 1.

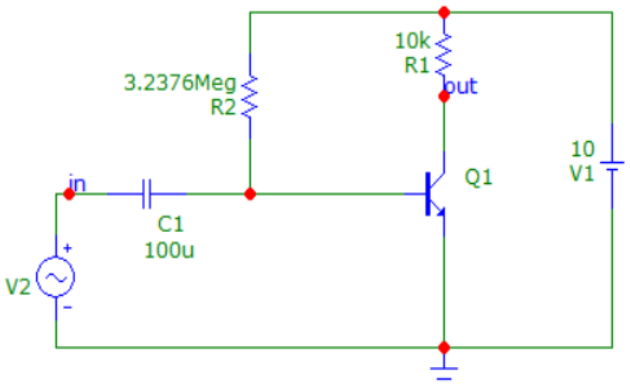


Рис. 1. Схема усилительного каскада с общим эмиттером

Принципиальная схема исследуемого усилителя содержит шесть элементов. Активным элементом служит биполярный транзистор Q1 типа 2N2219 структуры n-p-n.

Источник постоянного напряжения V1 величиной 10 В обеспечивает питание каскада. Источник V2 формирует входной синусоидальный сигнал частотой 60 Гц. Коллекторный резистор R1 сопротивлением 10 кОм преобразует изменения коллекторного тока в переменное выходное напряжение. Базовый резистор R2 номиналом 3,2376 МОм задаёт ток базы и фиксирует положение рабочей точки транзистора. Разделительный конденсатор C1 ёмкостью 100 мкФ пропускает переменную составляющую сигнала от генератора V2 на базу транзистора и блокирует постоянное напряжение смещения, препятствуя его попаданию в цепь источника сигнала.

[1] Пасынков В. В., Чиркин Л. К., Шинков А. Д. Полупроводниковые приборы. 1981. С. 166.

Корректная работа усилителя переменного напряжения возможна только при правильно заданной рабочей точке транзистора в режиме покоя. Рабочая точка определяет значения постоянных напряжений и токов при отсутствии входного сигнала. В схеме с общим эмиттером оптимальным считается положение рабочей точки в середине линейного участка передаточной характеристики, что обеспечивает максимальный неискажённый размах выходного напряжения.

В исследуемой схеме рабочая точка задана резистором R2. В результате моделирования в режиме DC Analysis получены следующие параметры: напряжение коллектор-эмиттер Uкэ = 5 В, ток коллектора Iк = 0,5 мА. При напряжении питания 10 В напряжение на коллекторе составляет половину питания, что соответствует теоретической рекомендации для максимизации динамического диапазона.

Моделирование выполнялось в программе Micro-Cap, представляющей собой среду схемотехнического анализа, построенную на вычислительном ядре SPICE (Simulation Program with Integrated Circuit Emphasis)[2]. Использовался режим анализа переходных процессов (Transient Analysis). Параметры анализа задавались в диалоговом окне Transient Analysis Limits: максимальное время расчёта 50 мс, время начала вывода результатов 0 с, максимальный шаг по времени 50 мкс. Отображение сигналов производилось в двух раздельных графических окнах с автоматическим масштабированием по оси Y.

Выбор относительно крупного шага дискретизации сделан для демонстрации эффекта несинхронности осциллограммы.

Измерение параметров сигналов проводилось курсорным методом с использованием инструментов Peak и Valley. Размах сигнала определялся как разность между максимальным и минимальным значениями напряжения за период.

На вход каскада через разделительный конденсатор C1 подавался синусоидальный сигнал частотой 60 Гц и амплитудой 20 мВ. Размах входного сигнала от пика до пика составляет 40 мВ. Осциллограммы входного и выходного сигналов, полученные в результате моделирования, приведены на рис. 2.

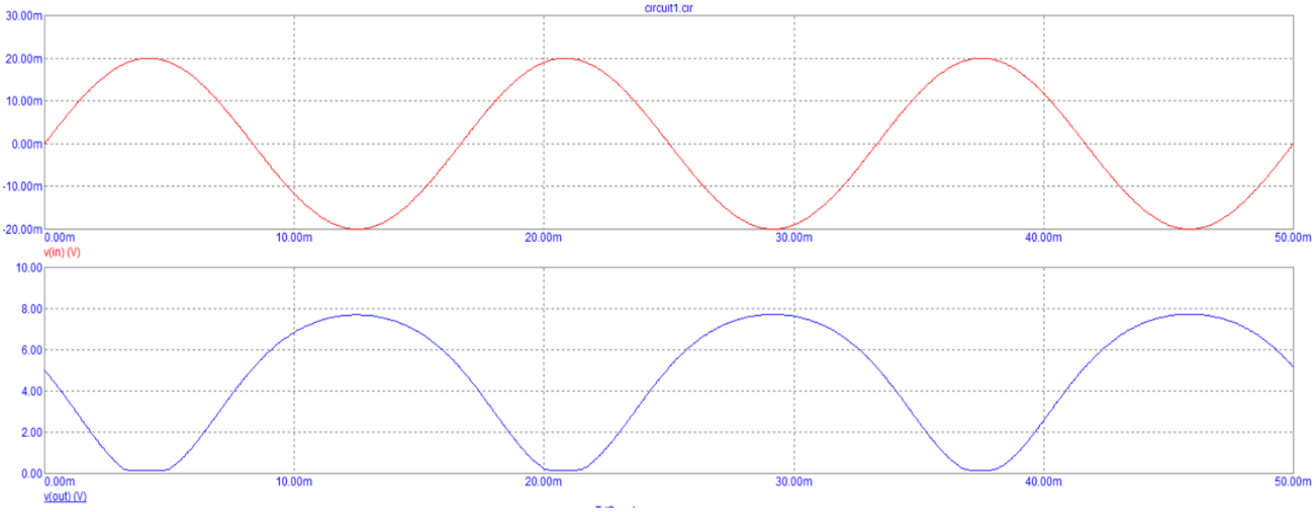


Рис. 2. Осциллограммы входного V(in) и выходного V(out) сигналов

Результаты измерения выходного сигнала в узле коллектора транзистора: максимальное значение напряжения 7,695 В, минимальное значение 0,126 В.

Размах выходного напряжения: Uвых(размах) = 7,695 В – 0,126 В = 7,569 В.

Коэффициент усиления по напряжению Ku определяется отношением размаха выходного сигнала к размаху входного:

Ku = 7569 мВ / 40 мВ = 189,2.

Полученное значение является типичным для каскада с общим эмиттером без отрицательной обратной связи и подтверждает высокие усилительные свойства данной схемы включения.

Осциллограмма выходного сигнала демонстрирует фазовый сдвиг 180° относительно входного: положительной полуволне входного напряжения соответствует отрицательная полуволна выходного. Инверсия фазы является фундаментальным свойством схемы с общим эмиттером и объясняется тем, что увеличение входного напряжения вызывает рост тока коллектора, увеличение падения напряжения на резисторе R1 и, как следствие, уменьшение напряжения на коллекторе относительно земли.

[2] Spectrum Software. Micro-Cap 12 Electronic Circuit Analysis Program: User's Guide. 12th ed. Sunnyvale, CA: Spectrum Software, 2018. URL: https://www.onsemi.com/pdf/datasheet/2n2219-d.pdf (дата обращения: 18.05.2026).

При уменьшении максимального шага по времени до 0,1 мкс осциллограмма становится гладкой и синхронной, что подтверждает исключительно вычислительную природу наблюдаемого эффекта.

В результате проведённого исследования усилителя переменного напряжения на биполярном транзисторе 2N2219, включённом по схеме с общим эмиттером, получены следующие результаты:

1. С помощью резистора R2 номиналом 3,2376 МОм задана рабочая точка транзистора: Uкэ = 5 В, Iк = 0,5 мА при напряжении питания 10 В.
2. При подаче на вход синусоидального сигнала частотой 60 Гц и размахом 40 мВ размах выходного сигнала составил 7,57 В.
3. Коэффициент усиления по напряжению Ku = 189.
4. Подтверждён инвертирующий характер каскада: выходной сигнал сдвинут по фазе на 180° относительно входного.

УДК 343.1:004(045)

С. А. Антипина,
обучающаяся 4 курса, «Юриспруденция»,
Институт права, социального управления и безопасности ФГБОУ ВО «УдГУ»,
И. А. Дубинин,
обучающийся 5 курса, «Правовое обеспечение национальной безопасности»,
Институт права, социального управления и безопасности ФГБОУ ВО «УдГУ».
Научный руководитель: Ф. А. Абашева, канд. юрид. наук, доцент
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Защита личности при использовании компьютерных технологий в уголовном судопроизводстве РФ

Развитие современных технологий меняет не только преступность, но и методы работы правоохранительных органов. Сегодня при осмотре места происшествия, обыске или допросе следователи все чаще используют фотоаппараты, видеокамеры и компьютерные программы для фиксации доказательств. Это позволяет точнее зафиксировать обстановку и детали, которые невозможно описать словами.

Однако действующие правила составления протокола следственного действия (ст. 166 УПК РФ) во многом остаются устаревшими и не учитывают особенности работы с цифровой информацией. На практике это приводит к серьезным сложностям.

Информационная безопасность личности – состояние защищённости человека от неправомерного воздействия на его информационную среду (несанкционированный доступ к персональным данным, нарушение тайны переписки, манипуляция сознанием). В правовом смысле это совокупность конституционных (ст. 23, 24 Конституции РФ) и отраслевых гарантий, обеспечивающих неприкосновенность частной жизни в цифровой сфере.

Ключевые критерии информационной безопасности применительно к защите личности в уголовном процессе:

1. **Законность** – соблюдение процедуры получения, фиксации и хранения цифровой информации, установленной УПК РФ и иными законами.
2. **Конфиденциальность** – неразглашение сведений, отсутствие несанкционированного доступа к данным.
3. **Целостность** – неизменность цифровой информации, подтверждённая (например, хэш-суммами) и зафиксированная в протоколе.
4. **Соразмерность (минимизация вмешательства)** – изъятие или копирование только того объёма данных, который необходим для расследования; сопутствующая информация (личная переписка не по делу) подлежит опечатыванию или удалению без просмотра.
5. **Доступность для уполномоченных субъектов** – легитимный доступ следователя, эксперта, суда к информации при сохранении её защиты от третьих лиц.
6. **Судебная контролируемость** – наличие в протоколе сведений, позволяющих суду проверить соблюдение прав личности при работе с цифровыми данными.

Указанные критерии производны от конституционных основ безопасности личности и должны быть имплементированы в содержание ст. 166 и 164.1 УПК РФ, а также в ведомственные инструкции.

Без их соблюдения технические средства фиксации не гарантируют защиты прав человека в цифровом судопроизводстве.

Легальную основу данного института составляют: Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 05.12.2016 № 646), а также нормы УПК РФ, регламентирующие порядок обращения с цифровыми доказательствами (в частности ст. 164.1).

В контексте уголовно-процессуальной деятельности и протоколирования следственных действий информационная безопасность личности приобретает особые черты. Следователь, изымая электронные носители или копируя цифровую информацию, получает доступ к данным, которые могут содержать сведения, не имеющие отношения к расследуемому преступлению, но являющиеся охраняемой законом тайной. Следовательно, обеспечение информационной безопасности в данном случае означает не только защиту доказательственной информации от искажения, но и защиту самой личности от необоснованного вмешательства в её частную жизнь.

Главная проблема заключается в следующем: закон разрешает использовать технические средства и приобщать к делу цифровые файлы, но не дает четких и понятных правил, как именно это нужно оформлять в протоколе. Нет единых требований к тому, как описывать видеофайлы, компьютерные данные, как проверять подлинность записи и как хранить такую информацию вместе с делом. Из-за этого возникают ошибки, которые в суде могут привести к тому, что важные доказательства признают недействительными только из-за неправильного оформления бумаг.

Как отмечает Б. Р. Ахметзянов, современный этап развития следственно-процессуальной деятельности характеризуется активным распространением достижений технического прогресса, что требует от следователя строгого соблюдения алгоритмической процедуры обнаружения и закрепления не только сведений о преступлении, но и материального или цифрового носителя этой информации[3].

Первой проблемой, требующей решения, является отсутствие единого понятийного аппарата. Как справедливо указывает Ю. И. Андреева, термины «электронный носитель», «цифровая информация», «электронные доказательства» зачастую трактуются правоприменителями по-разному[4]. П. С. Пастухов отмечает, что «электронные доказательства» в состязательной системе уголовно-процессуальных доказательств нуждаются в самостоятельном процессуальном статусе[5]. В. Е. Пономарев предлагает разграничивать «электронный носитель информации» и «цифровую информацию» как объект и содержание[6], а Н. Г. Яковлева вводит понятие «цифровые доказательства»[7]. Полагаю, что законодательное закрепление этих понятий позволит унифицировать практику составления протоколов.

Второй проблемой является шаблонность протоколов, составляемых с помощью технических средств. Л. Д. Калинкина на примере уголовных дел демонстрирует текстуальные совпадения разных процессуальных документов, что ставит под сомнение их доказательственное значение. Автор приходит к выводу, что использование технических средств не должно вести к формализму и обезличиванию протокола[8]. Разделяя эту позицию, считаю необходимым закрепить в ведомственных инструкциях требование об обязательном отражении в протоколе индивидуальных особенностей каждого следственного действия, недопустимости полного копирования шаблонов.

Третьей проблемой выступает обеспечение сохранности персональных данных и тайны следственного действия при использовании цифровых технологий. Б. Р. Ахметзянов обращает внимание, что при протоколировании изъятия электронных носителей возникает риск разглашения сведений, составляющих охраняемую законом тайну[9]. М. Р. Глушков указывает на соотношение протокола и технических средств фиксации, подчеркивая, что видеозапись или 3D-моделирование не заменяют,

---

[3] Ахметзянов Б. Р. Применение информационных цифровых технологий при протоколировании следственных действий // Гуманитарные, социально-экономические и общественные науки. 2026. № 2. С. 95–100.

[4] Андреева Ю. И. Электронные доказательства в уголовном процессе // Закон и право. 2025. № 8. С. 147–152.

[5] Пастухов П. С. «Электронные доказательства» в состязательной системе уголовно-процессуальных доказательств // Общество и право. 2015. № 1 (51). С. 192–196.

[6] Пономарев В. Е. Технико-криминалистическое обеспечение выявления и закрепления электронных доказательств : автореф. дис. ... канд. юрид. наук. Краснодар, 2025. 22 с.

[7] Яковлева Н. Г. Использование цифровых доказательств в уголовном судопроизводстве Российской Федерации // Вестник Тверского государственного университета. Серия «Право». 2024. № 4 (80). С. 117–126.

[8] Калинкина Л. Д. Изготовление протокола следственного действия с помощью технических средств: проблемы правоприменительной практики // Ученые записки кафедры уголовного процесса, правосудия и прокурорского надзора Мордовского государственного университета им. Н. П. Огарева. Саранск, 2017. Вып. 7. С. 25–28.

[9] Ахметзянов Б. Р. Применение информационных цифровых технологий при протоколировании следственных действий // Гуманитарные, социально-экономические и общественные науки. 2026. № 2. С. 95–100.

а дополняют письменный протокол[10]. С. Б. Россинский также отмечает, что протоколы следственных действий имеют проблемы процессуальной формы и доказательственного значения, которые не решаются простым добавлением технических приложений[11].

Таким образом, совершенствование порядка составления протокола следственного действия при применении технических средств и цифровых технологий должно идти по следующим направлениям:

1) законодательное закрепление единой терминологии в сфере электронных и цифровых доказательств;

2) соблюдение прав, свобод и законных интересов любого участника уголовного судопроизводства;

3) разработка процессуальных гарантий сохранности цифровой информации и соблюдения тайны следствия;

4) признание технических средств (включая 3D-моделирование и видеофиксацию) лишь дополнительным, но не заменяющим способом фиксации.

5) введение в протокол требования о соблюдении принципа «соразмерности цифрового вторжения» и фиксации мер по защите метаданных как элемента государственно-правовой охраны неприкосновенности частной жизни.

В контексте указанных проблем требует самостоятельного рассмотрения вопрос о понятийной определенности цифровых следов. Как отмечает группа авторов под руководством А. М. Багмета, цифровой след – это любая криминалистически значимая компьютерная информация, представленная в форме электрических сигналов, независимо от средств их хранения, обработки и передачи, которая относится к материальным невидимым следам. В. Б. Вехов, являясь одним из основоположников цифровой криминалистики в России, подчеркивает, что такие следы обладают двойственной природой: они одновременно имеют материальную форму (носитель) и информационное содержание, что отличает их от традиционных трасологических следов. Эта двойственность порождает сложности при процессуальном оформлении – следователь должен зафиксировать не только внешние признаки устройства, но и содержание хранящейся на нем информации, что действующим законодательством в полной мере не урегулировано.

Для углубленного анализа необходимо обратиться к государственно-правовым основам безопасности личности. Как отмечает Н. Н. Терехова, безопасность личности – межотраслевой институт на стыке конституционного, административного и информационного права. Ключевой фактор дестабилизации в постиндустриальном обществе – информационные угрозы, которые автор подразделяет на три уровня: угрозы психофизическому здоровью, неприкосновенности частной жизни и имущественного характера. Применительно к протоколированию следственных действий это означает, что неправильное оформление изъятия электронных носителей (шаблонность, отсутствие сведений о конфиденциальности) напрямую снижает уровень государственно-правовой защиты личности.

Кроме того, проблемой является недостаточный уровень специальных знаний у правоприменителей при работе с цифровыми следами. Исследователи в области криминалистической кибернетики указывают на противоречие между стремительным развитием технологических возможностей обработки цифровых данных и сохраняющимися нормативными ограничениями, а также недостаточной подготовкой кадров. Как обоснованно отмечается в научной литературе, современные следователи и эксперты часто не обладают достаточными компетенциями для использования современных информационных технологий, что приводит к неэффективному использованию имеющихся инструментов и снижает качество расследования преступлений.

Иным направлением является внедрение специализированных аппаратно-программных комплексов в практику осмотра места происшествия. А. А. Беляков и В. Ю. Иванов обосновывают необходимость применения таких комплексов, как «Мобильный криминалист» и UFED, которые позволяют извлекать информацию с заблокированных мобильных устройств, включая данные из облачных хранилищ и шифрованных приложений. Отдельные авторы отмечают, что при производстве всех следственных действий, связанных с изъятием носителей информации, должен присутствовать специалист в области компьютерной техники, обладающих определенными знаниями в сфере информационно-телекоммуникационных технологий, с тем, чтобы у других участников производства следственных действий не возникало сомнений в соблюдении закона.

---

[10] Глушков М. Р. О соотношении протокола и технических средств фиксации хода и результатов следственного действия // Проблемы правоохранительной деятельности. 2020. № 4. С. 16–20.

[11] Россинский С. Б. Протоколы следственных действий: проблемы процессуальной формы и доказательственного значения // Lex Russica. 2017. № 10 (131). С. 36–46.

Не менее значимой является проблема фиксации цифровых следов, находящихся в облачных хранилищах и на удаленных серверах. А. В. Земскова и С. С. Минаков обращают внимание на то, что правоприменительная практика выявила новые актуальные проблемы следственных действий, обусловленные широким внедрением облачных технологий обработки информации, виртуализацией вычислений и инфраструктуры. Авторы задаются принципиальным вопросом: если компьютерная система распределена в «облачной» инфраструктуре, что именно и как следует осматривать и изымать в соответствии с УПК РФ? Этот вопрос требует законодательного решения, поскольку действующие нормы ориентированы на изъятие физических носителей, тогда как цифровая информация все чаще хранится на серверах, расположенных в иных юрисдикциях.

Наконец, в контексте обеспечения допустимости цифровых доказательств особого внимания заслуживает вопрос о применении методов криптографической защиты. Н. Н. Михайлов отмечает, что важное значение имеет статья 164.1 УПК РФ, закрепляющая особенности изъятия электронных носителей информации и копирования с них данных, однако на практике сохраняются сложности с обеспечением целостности цифровых следов на всех этапах их обработки. Исследователи в области криминалистической кибернетики предлагают использовать хэширование и блокчейн-технологии для фиксации момента создания или изменения цифрового следа, что позволит в дальнейшем подтвердить его неизменность в суде.

В развитие темы защиты личности Н. Н. Терехова анализирует механизмы реализации права на неприкосновенность частной жизни (ст. 23 Конституции РФ) и приходит к выводу о недостаточности традиционных процессуальных гарантий в условиях цифрового оборота данных. Автор обосновывает принцип «соразмерности цифрового вторжения»: любое следственное действие должно содержать в протоколе обоснование неизбыточности изымаемых сведений. Особое внимание Н. Н. Терехова уделяет защите метаданных (геолокация, время соединений, данные о звонках) как самостоятельному объекту правовой охраны. С учетом этого полагаем, что протокол следственного действия должен разграничивать информацию доказательственного значения и сопутствующие цифровые данные, подлежащие опечатыванию или удалению без просмотра[12].

Реализация предложенных мер позволит повысить доказательственное значение протоколов следственных действий, обеспечить баланс между использованием современных технологий и соблюдением процессуальных гарантий, а также сформировать единообразную и непротиворечивую следственную практику в условиях цифровизации уголовного судопроизводства. Как резюмирует Н. Н. Терехова, безопасность личности в информационной сфере требует не только технических, но и системных процессуальных решений – в первую очередь в институте протоколирования следственных действий.

УДК 621.31:004.056(045)

Э. Р. Ахиярова,
обучающаяся 2 курса Института права,
социального управления и безопасности ФГБОУ ВО «УдГУ».
Научный руководитель: Т. Н. Стерхова, канд. техн. наук, доцент
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Сравнительный анализ требований ФСТЭК России и стандарта NIST (США) к обеспечению безопасности в электроэнергетике

Тема кибербезопасности в электроэнергетике сейчас звучит острее, чем когда-либо. Речь идёт не просто о защите данных, а о работающих электростанциях, линиях электропередачи и системах управления, от которых зависит жизнь целых регионов. В России и США – двух технологических лидерах – сложились разные подходы к этой проблеме. С одной стороны, жёсткое государственное регулирование, с другой – гибкие рекомендательные стандарты. Сопоставить их, понять сильные и слабые стороны каждой модели – задача не только научная, но и очень практическая. Особенно

[12] Терехова Н. Н. Государственно-правовые основы безопасности личности в Российской Федерации. М. : Наука, 2009. 212 с.

если учесть, что в России с сентября 2024 года начал действовать новый приказ Минэнерго № 1215, а в США обновили версию ключевого стандарта NIST SP 800-82.

В основе нашей системы – Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры». Главный надзорный орган – ФСТЭК России, которая прописывает довольно жёсткие правила для автоматизированных систем управления технологическими процессами (АСУ ТП). Отдельного внимания заслуживает приказ Минэнерго № 1215 от 26 декабря 2023 года. Он вступил в силу 1 сентября 2024 года и вносит дополнительные требования именно для электроэнергетики, причём в части дистанционного управления технологическими режимами.

Требования распространяются на дистанционное управление: выключателями, разъединителями, заземляющими разъединителями, технологическим режимом работы электросетевого оборудования и устройствами релейной защиты и автоматики; активной и реактивной мощностью: генерирующего оборудования ветровых и солнечных электростанций, а также гидравлических электростанций установленной генерирующей мощностью менее 50 МВт; активной мощностью: гидравлических и гидроаккумулирующих электростанций, а также тепловых электростанций.

Среди основных технических требований можно выделить: защиту управляющего трафика – для передачи команд между диспетчерским пунктом, энергообъектами и центром управления сетями в локальной сети объекта применяются виртуальные локальные сети (VLAN), а сам трафик подлежит криптографической защите. Изоляция технологических сетей – категорически запрещается доступ из сети «Интернет» в сегмент технологических сетей связи, через который осуществляется дистанционное управление. Межсетевое экранирование – взаимодействие технологических сетей, задействованных в дистанционном управлении, с внешними выделенными сетями связи должно быть организовано исключительно через межсетевой экран. Контроль целостности передаваемых команд – в отношении программного обеспечения, применяемого для дистанционного управления из диспетчерских центров, должны быть реализованы следующие процедуры: отслеживание, выявление и устранение ошибок и уязвимостей ПО; установление порядка и сроков информирования пользователей разработчиками (производителями) об обнаруженных уязвимостях; определение компенсирующих защитных мер либо ограничений по использованию ПО; разъяснение пользователям способов получения обновлений, а также методов проверки их подлинности и целостности[13].

Американский подход к регулированию кибербезопасности в энергетике базируется на рекомендательных стандартах, обеспечивающих организациям гибкость в выборе мер защиты. Ключевым документом для промышленных систем управления (Industrial Control Systems, ICS) является NIST Special Publication 800-82.

NIST SP 800-82, rev. 3 (безопасность операционных технологий**):** широко распространенный документ, в котором архитектура безопасности, средства контроля и методы управления жизненным циклом адаптированы для промышленных сред, где безопасность и доступность важнее конфиденциальности. В нем особое внимание уделяется сегментации, принципу предоставления минимальных привилегий, надежному, но защищенному удаленному доступу и непрерывному мониторингу, адаптированному для операционных сред[14].

Ключевые требования подхода: Согласно требованиям Национального института стандартов и технологий США, операторы должны изолировать контрольные зоны, обеспечивать маршрутизацию с минимальными привилегиями и пропускать трафик через контролируемые демилитаризованные зоны, чтобы ограничить горизонтальное перемещение. В редакции 3 вводятся требования о многофакторной аутентификации, аудите хостов-переходов и ограничении срока действия учетных записей подрядчиков для любых способов удаленного обслуживания систем промышленной автоматизации. В руководстве ужесточаются требования к проверке с учетом протоколов, инвентаризации активов и ведению журналов с синхронизацией по времени, чтобы службы реагирования могли восстанавливать картину инцидентов в сфере промышленной автоматизации[15].

Важный нюанс: в американской электроэнергетике, помимо добровольного NIST, применяются ещё и обязательные стандарты NERC CIP (Critical Infrastructure Protection). Они устанавливают минимальный уровень управления рисками для идентификации активов, контроля доступа, реагирования на инциденты и проверки цепочки поставок. Правда, они охватывают не всех: распределительные сети

[13] О дистанционном управлении объектами электроэнергетики : приказ Минэнерго России № 1215 от 26.12.2023 // СПС «Гарант». URL: https://www.garant.ru/products/ipo/prime/doc/408930964/ (дата обращения: 04.04.2026).

[14] NIST Special Publication 800-82 Revision 3. Guide to Operational Technology (OT) Security // NIST. URL: https://www.edmi-meters.com/ (дата обращения: 04.04.2026).

[15] Ключевые требования NIST SP 800-82 rev. 3 к сегментации и мониторингу ICS // ZephTech. URL: https://zephtech.net/feed/2025-10-22-nist-ics-segmentation (дата обращения: 04.04.2026).

и мелкие муниципальные компании могут попадать под них не в полной мере. Тем не менее именно NERC CIP вносит в американскую систему элемент принудительности, которого нет в чистом NIST[16].

Главное различие между подходами ФСТЭК и NIST лежит в плоскости «жесткого» и «мягкого» регулирования. Российская система является императивной и предписывающей. Она основана на выполнении конкретных, детализированных требований, зафиксированных в приказах и методических документах. Субъекты КИИ обязаны выполнять эти требования, а регулятор осуществляет контроль за их исполнением. Подход NIST, напротив, является рекомендательным и риск-ориентированным. Организации сами решают, какие риски для них важны, и подбирают меры защиты под себя, пользуясь готовыми каталогами вроде NIST SP 800-53, где вариантов очень много. Главное удобство в том, что меры там уже расставлены по приоритетам: можно сначала внедрить самое важное и получить максимум пользы, даже если бюджет и ресурсы ограничены.

Хотя подходы в России и США различаются, общие приоритеты все равно присутствуют. Во-первых, и у нас, и у них требуется изолировать управляющие сети от интернета и публичных сетей. Во-вторых, оба стандарта особенно строго следят за тем, чтобы удаленное управление было безопасным. В-третьих, нужно следить за целостностью передаваемых команд и данных. В-четвертых, надо обязательно внедрять системы обнаружения атак. А также никуда без четкого учета всего оборудования и программного обеспечения.

Подведя итоги, можно сказать, что Россия выбрала жесткую модель, в которой правила прописаны до мелочей. США же стали применять более гибкую модель, где стандарты NIST – это скорее рекомендации, и каждая компания сама решает, что ей подходит. При этом сходства тоже есть. Везде нужны сегментация сети, защита удаленного доступа, контроль целостности, мониторинг инцидентов и учет активов. Также есть особенности российского подхода, которые не имеют аналогов в американской системе: переход на отечественное ПО, подключение к ГосСОПКА, а также государство само решает, какие объекты КИИ считать типовыми. Российский подход обеспечивает высокую управляемость и имеет единые стандарты, но есть недостаток – дорогое импортозамещение. Американский подход предоставляет организациям самим выбрать, как защищаться, но нужен высокий уровень зрелости в управлении рисками.

УДК 004.056:004.7

Н. А. Баязитов,
обучающийся 3 курса Института права,
социального управления и безопасности ФГБОУ ВО «УдГУ».
Научный руководитель: Т. Н. Стерхова, канд. техн. наук, доцент
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Анализ угроз доверенных USB HID-устройств на примере демонстрационного макета

Интерфейс USB сегодня является основным способом подключения периферийных устройств к вычислительным системам. Его широкое распространение связано с поддержкой технологии Plug & Play, благодаря которой устройство автоматически распознаётся после подключения.

Среди USB-устройств особое место занимает класс HID (Human Interface Device), к которому относятся клавиатуры, мыши и другие устройства ввода. Такие устройства автоматически определяются операционной системой и считаются доверенными.

Однако механизм автоматического доверия может использоваться как потенциальный источник угроз. Если устройство программно эмулирует клавиатуру, операционная система воспринимает его как легитимное HID-устройство и принимает ввод без дополнительной проверки.

Целью данной работы стало исследование принципов функционирования HID-устройств, создание демонстрационного устройства на базе микроконтроллера ATmega32U4 и анализ связанных с этим угроз информационной безопасности.

[16] Стандарты NERC CIP для энергетического сектора // EDMI. URL: https://www.edmi-meters.com/ (дата обращения: 04.04.2026).

После подключения USB-устройства операционная система запускает процедуру инициализации – enumeration. Во время этого процесса устройство передаёт системе сведения о своём типе, классе и поддерживаемых функциях[17].

На основе полученных данных ОС автоматически загружает драйвер и начинает взаимодействие с устройством.

Класс HID включает:

- клавиатуры;
- мыши;
- игровые контроллеры;
- другие устройства ввода.

Особенностью HID является отсутствие необходимости установки специализированных драйверов. Поддержка данного класса встроена в операционные системы, что обеспечивает мгновенную готовность устройства к работе.

Основная проблема безопасности заключается в том, что система не проверяет, является ли устройство настоящей клавиатурой. Если устройство корректно реализует HID-протокол, оно получает возможность отправлять команды от имени пользователя[18].

Для реализации демонстрационного устройства использовалась плата Arduino Pro Micro на базе микроконтроллера ATmega32U4.

Данный микроконтроллер обладает встроенным USB-контроллером, позволяющим напрямую реализовывать HID-функциональность без дополнительных преобразователей интерфейсов.

Преимущества выбранной платформы:

- встроенная поддержка USB;
- компактность;
- простота программирования;
- поддержка HID-эмуляции.

Использование готовой платы позволило отказаться от разработки собственной электронной схемы и сосредоточиться непосредственно на исследовании вопросов информационной безопасности. После подключения устройство автоматически определялось системой как HID-клавиатура.

Программная реализация выполнялась в среде разработки Arduino IDE с использованием библиотеки Keyboard.h[19].

Библиотека Keyboard позволяет эмулировать нажатия клавиш, отправлять текстовые данные и использовать системные комбинации клавиш.

Алгоритм работы программы:

1) подключение устройства;
2) ожидание завершения инициализации системы;
3) запуск HID-интерфейса;
4) выполнение сценария автоматического ввода.

В рамках демонстрационного сценария устройство после подключения автоматически открывало текстовый редактор и выполняло ввод заранее подготовленного текста. При этом все действия воспринимались системой как обычный пользовательский ввод с клавиатуры.

Особенность HID-устройств состоит в высоком уровне доверия со стороны операционной системы. Это создаёт возможность автоматизированного выполнения различных действий без непосредственного участия пользователя. Подобный принцип используется в атаках класса BadUSB, основанных на подмене функциональности USB-устройств.

Потенциальные риски:

- автоматический ввод команд;
- запуск приложений;
- изменение пользовательских настроек;
- выполнение действий от имени пользователя.

При этом подобные устройства не используют уязвимости ОС, не требуют установки программ и взаимодействуют с системой через штатный интерфейс.

---

[17] Жуков А. Гадкий утенок. Превращаем обычную флешку в USB Rubber Ducky. URL: https://xakep.ru/2015/09/11/usb-rubber-ducky/ (дата обращения: 21.03.2026).

[18] Злой HID. Делаем и программируем хакерский девайс для HID-атак. URL: https://xakep.ru/2018/09/26/evil-hid/ (дата обращения: 21.03.2026).

[19] BadUSB: Эксперименты с Arduino и Flipper Zero. URL: https://habr.com/ru/articles/767996/ (дата обращения: 21.03.2026).

Основным условием реализации подобных сценариев является физический доступ к устройству.

В ходе эксперимента устройство было подключено к компьютеру с операционной системой Windows 11 (см. рис. 1).

Рис. 1. Подключение устройства

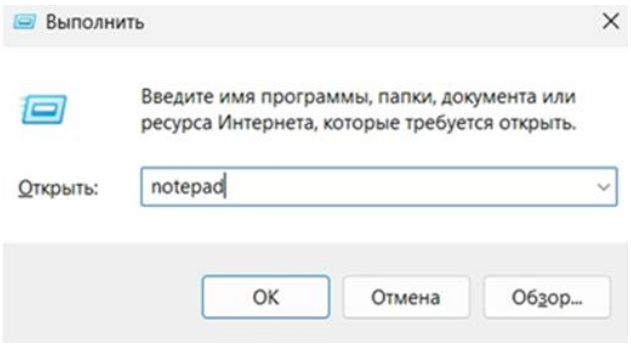


Рис. 2. Выполнение комбинации клавиш Win+R и запуск блокнота

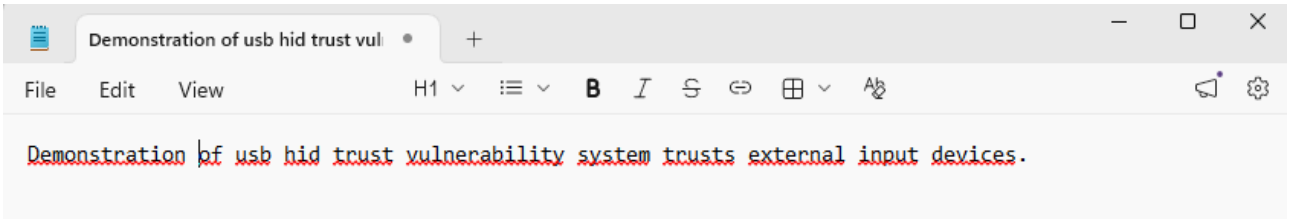


Рис. 3. Вписывание заданного текста

Результаты показали:

- успешное определение устройства как HID-клавиатуры;
- автоматическую установку драйвера;
- корректное выполнение сценария (см. рис. 2, 3);
- отсутствие блокировки со стороны встроенных средств защиты.

Также было установлено, что стабильность работы зависит от временных задержек и особенностей конфигурации системы.

Проведённый эксперимент подтвердил возможность практической реализации HID-эмуляции с использованием доступных микроконтроллеров.

Для снижения рисков рекомендуется применение комплекса защитных мер:

- ограничение использования USB-портов;
- применение Device Control;
- использование белых списков устройств;
- контроль HID-подключений;
- физическая защита рабочих станций;
- обучение пользователей.

В корпоративной среде также используются системы Endpoint Protection и политики групповой безопасности[20].

В ходе работы были изучены особенности работы USB HID-устройств, а также рассмотрены возможные угрозы информационной безопасности, связанные с их использованием. Исследование показало, что современные микроконтроллеры с поддержкой USB позволяют реализовывать HID-эмуляцию без применения сложного оборудования или специализированных аппаратных средств.

Главная проблема заключается в том, что операционная система изначально доверяет HID-устройствам. Из-за этого контроль подключаемой периферии становится важной частью обеспечения информационной безопасности.

[20] Щербаков Ю. Новая угроза BadUSB и подходы к защите. URL: https://ib-bank.ru/bisjournal/post/424 (дата обращения: 10.04.2026).

УДК 621.313.333(045)

А. Д. Бояршинова, И. Э. Рахимов,
обучающиеся 3 курса Института права,
социального управления и безопасности ФГБОУ ВО «УдГУ».
Научный руководитель: Т. Н. Стерхова, канд. техн. наук, доцент
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Исследование трёхфазного короткозамкнутого асинхронного двигателя

Асинхронные электродвигатели, особенно с короткозамкнутым ротором, являются наиболее массовыми потребителями электрической энергии в промышленности и сельском хозяйстве благодаря простоте конструкции, высокой надежности и низкой стоимости. Понимание физических процессов, происходящих при преобразовании электрической энергии в механическую, а также умение экспериментально определять и анализировать рабочие характеристики двигателя (зависимости P1, I1, n2, cosφ, η, s, M = f(P2)) является основой грамотной эксплуатации и выбора электрооборудования[21]. Для современного производства необходимо владеть конкретной, проверенной экспериментальным путем, информацией о коэффициенте полезного действия и коэффициенте мощности трёхфазного короткозамкнутого асинхронного двигателя при различных нагрузках.

Цель работы – изучить устройство и принцип работы трёхфазного асинхронного двигателя с короткозамкнутым ротором, практически изучить основные рабочие характеристики, рассчитать энергетические параметры, основываясь на опытных данных и схеме замещения.

Среди различных видов электродвигателей на производствах чаще всего используются именно асинхронные электродвигатели. Столь высокая распространенность связана с простотой конструкции, достаточно высоким уровнем надёжности и прочности, а также существенно сниженной стоимостью, по сравнению с иными типами электродвигателей. При условии широкой распространенности асинхронных трёхфазных короткозамкнутых двигателей экспериментальный анализ определения их характеристик остается всё так же востребован, как студентами в процессе обучения, так и инженерами на предприятиях. Обусловлена эта необходимость в первую очередь влиянием хода времени и условий эксплуатации и хранения на комплексные изделия. Фактические показатели, ввиду вышеупомянутых и других факторов, могут различаться с описанными в документации на двигатели.

Испытание проходило с использованием трёхфазного асинхронного двигателя с короткозамкнутой обмоткой ротора (рис. 1). Отсутствие скользящих контактов делает данный тип машин особенно устойчивым к износу[22].

В процессе работы было осуществлено четыре последовательных пуска при различных величинах нагрузочного сопротивления в цепи якоря генератора, что соответствовало разным значениям тока нагрузки I_2.

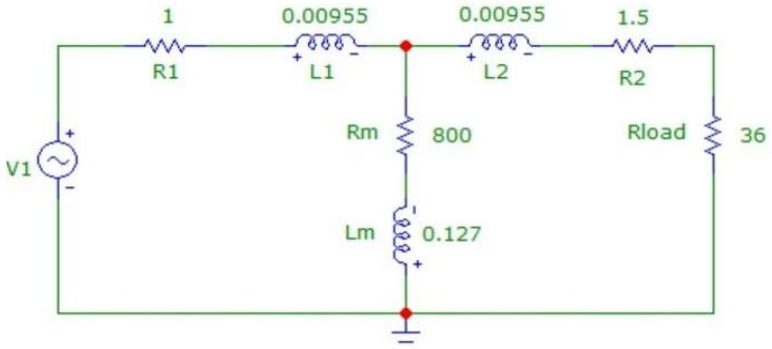


Рис. 1. Схема подключения асинхронного короткозамкнутого электродвигателя

Скольжение S, характеризующее относительное отставание ротора от вращающегося магнитного поля, определялось по известному выражению[23]: $S=((n_1-n)/n_1)100\%$, где n_1=1500 об/мин – скорость вращения магнитного поля статора.

[21] Иванов-Смоленский А. В. Электрические машины: учебник для вузов. М. : Энергия, 1980. С. 229.
[22] Копылов И. П. Электрические машины : учебник для вузов, 4 изд., перераб. и доп. М. : Высш. школа, 2012. С. 264.
[23] Брускин Д. Э., Зорохович А. Е., Хвостов В. С. Электрические машины : в 2 ч. Ч. 1. М. : Высш. школа, 1987. С. 215.

Полезная механическая мощность на валу P_2 вычислялась через электрическую мощность генератора постоянного тока, выступающего в роли тормоза, с учётом коэффициента полезного действия передачи[24]: $P_2=0{,}65P_{торм}=0{,}65\ I_2\ U_2$

Коэффициент полезного действия испытуемой машины находился как отношение отдаваемой мощности к потребляемой из сети: $\eta=(P_2/3P_{1ф})100\%$, где $P_{1ф}$ – активная мощность, потребляемая одной фазой статора.

В таблице 1 сведены непосредственно измеренные величины, а также результаты выполненных расчётов для четырёх характерных точек нагрузки – от режима, близкого к идеальному холостому ходу, до режима значительного торможения.

Таблица 1

Сводные данные испытаний асинхронного двигателя

U, В	I_1, А	P_1, кВт	I_2, А	n, об/мин	M, Н·м	P_2, кВт	cosφ	η, %	s
380	0,85	0,15	0	1498	0	0	0,26	0	0,001
380	9,17	6,3	0.5	1440	54,8	8,27	0,85	85	0,04
380	28,3	14	1.0	1304	170	23,2	0,75	80	0,131
380	41,5	17,8	2.0	1154	214	25,8	0,65	70	0,231

Анализ полученных данных позволяет наглядно проследить классические закономерности, присущие асинхронным машинам. По мере увеличения механической нагрузки на валу происходит закономерное снижение оборотов и рост скольжения. В четвёртом опыте частота упала до 1154 об/мин, что соответствует скольжению более 23 %. Следует отметить, что рабочий диапазон двигателя ограничен критическим скольжением, превышение которого приводит к «опрокидыванию» – резкому падению момента и остановке.

Полученные графические зависимости (представлены на рисунках 2–6) имеют типовой вид для асинхронных машин общепромышленной серии, что подтверждает корректность проведённых измерений и работоспособность лабораторного оборудования.

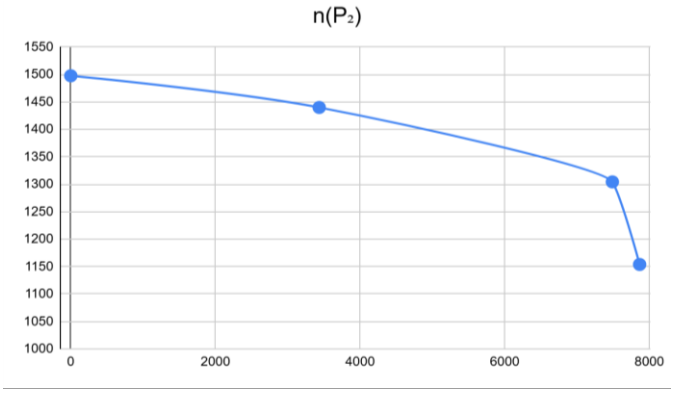


Рис. 2. Графики зависимости частоты вращения и коэффициента скольжения от мощности на валу

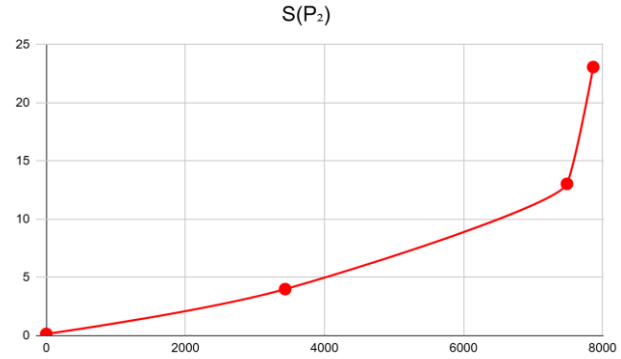


Рис. 3. Графики зависимости частоты вращения и коэффициента скольжения от мощности на валу

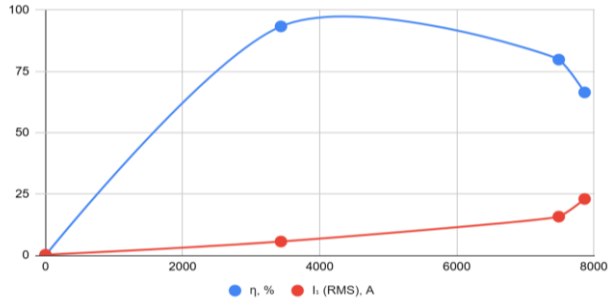


Рис. 4. График зависимости тока статора и КПД от мощности на валу

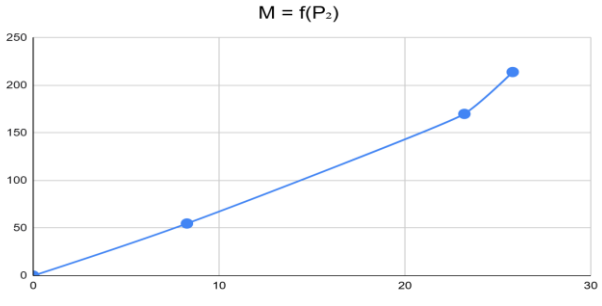


Рис. 5. График зависимости Момента от мощности на валу

[24] Кацман М. М. Электрические машины : учебник для студ. учреждений сред. проф. образования. 13 изд., стер. М. : Изд. центр «Академия», 2014. С. 245.

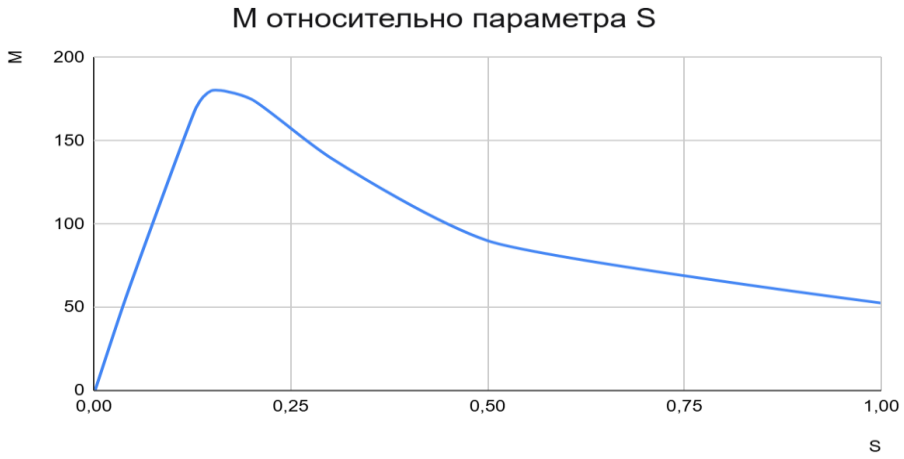


Рис. 6. График зависимости Момента от скольжения

В результате проведённого лабораторного исследования определены и проанализированы основные рабочие характеристики трёхфазного асинхронного двигателя с короткозамкнутым ротором. Экспериментально подтверждено, что с ростом механической нагрузки на валу увеличиваются потребляемый ток и скольжение, при этом частота вращения снижается. Зависимость коэффициента полезного действия имеет ярко выраженный максимум в зоне номинальных нагрузок. Полученные навыки расчёта параметров и анализа режимов работы асинхронной машины могут быть использованы при выполнении курсовых проектов по электромеханике и при решении прикладных задач выбора электропривода.

УДК 621.3.08:614.7/8:004(045)

К. А. Булдаков, Д. В. Логинов,
обучающиеся 2 курса Института права,
социального управления и безопасности ФГБОУ ВО «УдГУ».
Научный руководитель: Т. Н. Стерхова, канд. техн. наук, доцент
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Анализ мобильных приложений для измерения электромагнитного поля

В последнее время население обеспокоено электромагнитной безопасностью жилых помещений. Одновременно с этим в магазинах приложений появились множество программ, якобы позволяющих измерить «опасное электромагнитное излучение» от бытовой техники. Актуальность исследования обусловлена не только метрологической проблемой, но и аспектами информационной безопасности: распространение недостоверных измерительных приложений создаёт риск введения пользователей в заблуждение, формирования ложных представлений об электромагнитной обстановке и, как следствие, принятия неверных решений в области безопасности. Санитарной нормой принято предельно допустимое значение переменного магнитного поля промышленной частоты 50 Гц для жилых помещений – 0,5 мкТл (СанПиН 1.2.3685–21)[25]. Заметим, что датчик телефона измеряет только постоянное магнитное поле (включая поле Земли, которое приблизительно равно 40–50 мкТл), поэтому принципиально не способен правильно измерить переменное поле 50 Гц. Однако, оценка поведения приложений при приближении к источникам и стабильность показаний позволяют судить о точности измерений и потенциальной полезности для учебных задач. Цель работы – исследовать точность трёх популярных мобильных приложений для измерения магнитного поля и выявление их пригодности для реального мониторинга результатов.

[25] СанПиН 1.2.3685-21 «Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания». URL: https://nagut6.gosuslugi.ru/netcat_files/174/2801/SP123685_21.pdf (дата обращения 10.04.2026).

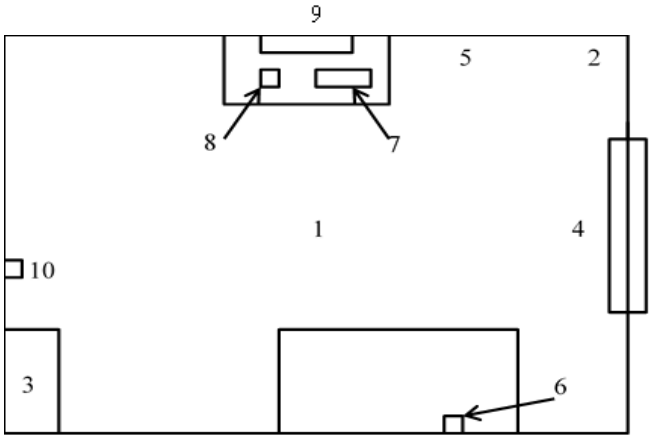
Для исследования были выбранны приложения «Magnetometer[26]», «EMF Detector[27]» и «Physics Toolbox Suite[28]». Выбор обусловлен тем, что все приложения находятся в открытом доступе. Измерения проводились в 10 точках жилой комнаты № 1 (см. рис. 1) и 10 точках жилой комнаты № 2 (см. рис. 1). Показания приложений записывались по трём осям (X, Y, Z в мкТЛ), после чего вычислялось среднее арифметическое значение для анализа. Фоновые точки (1–5) располагались вдали от электроприборов, а точки 6–10 – вблизи работающих источников.

Результаты эксперимента представлены в таблицах 1 и 2. В комнате № 1 все три приложения показали фоновые значения около 44–47 мкТл, что соответствует магнитному полю Земли. Приближение к работающим приборам вызывало различную реакцию. Приложение «Magnetometer» продемонстрировало логичный рост: от 44,5–45,3 мкТл (фон) до 62,83 мкТл у телевизора; среднее по 10 точкам – 50,25 мкТл. «EMF Detector» выдало аномально высокий фон в точке 3 (51,17 мкТл) при отсутствии источников и нелогичное снижение у ноутбука (48,50 мкТл) по сравнению с фоном; среднее – 51,89 мкТл. «Physics Toolbox» показало наиболее стабильный фон (44,63–45,20 мкТл) и плавный рост у источников (до 60,83 мкТл у телевизора); среднее – 49,47 мкТл. Аналогичная картина наблюдалась в комнате №2, где присутствовал мощный системный блок: «Physics Toolbox» дал рост с 44,73–45,30 мкТл (фон) до 64,83 мкТл, тогда как «EMF Detector» зафиксировал скачок до 70,50 мкТл, не согласующийся с показаниями других приложений.

Таблица 1

Сравнение средних значений магнитного поля (мкТл) в комнате № 1

Приложение	Фон (среднее)	Рядом с телевизором	Общее среднее
Magnetometer	44,9	62,83	50,25
EMF Detector	46,6	65,50	51,89
Physics Toolbox	44,9	60,83	49,47



1. Центр комнаты
2. Угол
3. Шкаф
4. Подоконник
5. Стена
6. Розетка с зарядкой телефона
7. Удлинитель с ноутбуком
8. Блок питания ноутбука
9. Телевизор
10. Выключатель света

Рис. 1. План комнаты № 1

Таблица 2

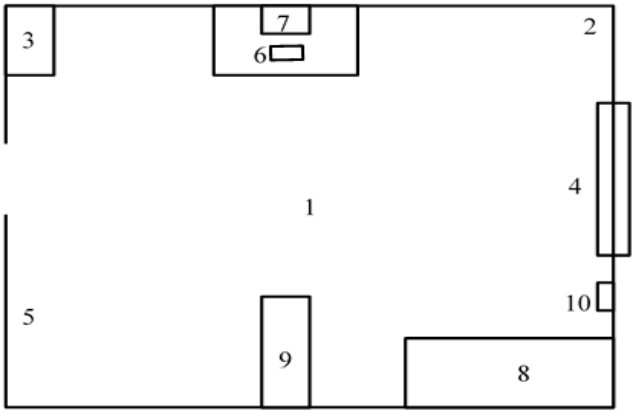
Сравнение средних значений магнитного поля (мкТл) в комнате № 2

Приложение	Фон (среднее)	Рядом с системным блоком	Общее среднее
Magnetometer	45,0	65,83	50,29
EMF Detector	46,6	70,50	52,95
Physics Toolbox	45,0	64,83	49,83

[26] Magnetometer – приложение от Smart Tools Co. URL: https://www.rustore.ru/catalog/app/com.appdevgenie.magnetometer (дата обращения: 10.04.2026).

[27] EMF Detector – EMF Meter от AntiqueApp. URL: https://play.google.com/store/apps/details?id=com.zeehikitzon.emfdetector.emfmeter.radiationdetector&hl=ru (дата обращения: 10.04.2026).

[28] Physics Toolbox Suite. URL: https://play.google.com/store/apps/details?id=com.chrystianvieyra.physicstoolboxsuite (дата обращения: 10.04.2026).



1. Центр комнаты
2. Угол
3. Шкаф
4. Подоконник
5. Стена
6. Розетка с зарядным устройством
7. Блок питания компьютера
8. Кровать
9. Телевизор
10. Розетка

Рис. 2. План комнаты № 2

Сравнение приложений (см. рис. 1, 2) позволило сделать выводы: Приложение «Magnetometer» честно считывает данные с магнитометра, прост в использовании, но имеет малый функционал. «EMF Detector» выдал самые неточные значения: его показания хаотичны, нестабильны, также значения отличаются от других приложений. «Physics Toolbox» признан наиболее рабочим приложением благодаря высокой точности, логичной реакции на источники (как видно на рис. 1 и 2, в точках 6–10) и благодаря большому инструментарию, хоть и интерфейс приложения является не самым удобным. Однако все три приложения показывают значения, примерно в 100 раз превышающие санитарную норму для переменного поля, что объясняется измерением постоянного поля Земли. Следовательно, ни одно приложение толком не пригодно для оценки электромагнитной безопасности бытовых приборов переменного поля 50 Гц.

Таким образом, доверие мобильным приложениям для измерения электромагнитного поля от розеток и бытовой техники необоснованно. Для реальной оценки электромагнитной обстановки необходимо использовать профессиональные измерительные приборы. «Physics Toolbox» и аналогичные приложения целесообразно применять только в учебных целях, зная факт чёткого понимания их ограничений.

УДК 004.94:61(045)

Н. А. Бычков,
обучающийся 2 курса Института права,
социального управления и безопасности ФГБОУ ВО «УдГУ».
Научный руководитель: Т. Н. Стерхова, канд. техн. наук, доцент
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Разработка программного модуля для имитационного моделирования диагностических процедур

Современное медицинское образование требует от студентов не только теоретических знаний, но и практических навыков работы с диагностическим оборудованием. Однако доступ к лабораторной базе, расходным материалам и приборам часто ограничен по времени и ресурсам. Особенно остро эта проблема стоит при изучении методов исследования функции внешнего дыхания (ФВД), где требуется не только понимание физиологических процессов, но и умение интерпретировать показания приборов в реальном времени. Одним из путей решения данной проблемы является применение технологий имитационного моделирования, позволяющих воссоздать работу диагностической аппаратуры и реакцию биологических систем в виртуальной среде[29].

К числу основных методов оценки ФВД относятся пикфлоуметрия – измерение пиковой скорости выдоха (ПСВ), и пневмотахометрия – оценка объёмной скорости воздушного потока на вдохе и выдохе. Указанные методы широко применяются для диагностики бронхиальной астмы, хрониче-

[29] Анохин М. Компьютерная спирометрия у детей. М. : Бином, 2012. С. 104.

ской обструктивной болезни лёгких и других респираторных нарушений. Принципы работы данных методов подробно изложены в фундаментальных руководствах по физиологии человека[30], а применение компьютерной спирометрии освещено в специализированной литературе[31].

В данной работе описывается разработка программного модуля «LEARN PHYSIOLAB», включающего пять тренажёров по физиологии, с акцентом на модули оценки функции внешнего дыхания: пикфлоуметрию и пневмотахометрию. Новизна работы заключается в применении реальных статистических данных, полученных при инструментальном обследовании студентов, для построения математической модели симулятора. Идея создания программы возникла при взаимодействии со студентами Ижевского государственного медицинского университета (ИжГМУ), которым требовался удобный инструмент для отработки лабораторных навыков вне стен академии.

Материалы и методы: Программный модуль реализован на языке Python с использованием фреймворка Flet, обеспечивающего создание кроссплатформенного графического интерфейса. Выбор Python обусловлен его распространённостью в академической среде и доступностью инструментов для численных расчётов и визуализации данных. Фреймворк Flet позволяет создавать настольные приложения с минимальными требованиями к аппаратному обеспечению, что важно для использования в учебных аудиториях.

Для построения математической модели пневмотахометра проведены натурные измерения показателей функции внешнего дыхания у 20 студентов Ижевского государственного медицинского университета (ИжГМУ). Измерения выполнялись с использованием сертифицированного медицинского прибора – пневмотахометра. Для каждого испытуемого фиксировались максимальная объёмная скорость (МОС) на вдохе и объём форсированного выдоха за первую секунду (ОФВ1).

В выборку вошли мужчины (n=7), женщины (n=8) и спортсмены (n=5). У мужчин зафиксированы следующие диапазоны: МОС вдоха – от 6,5 до 9,0 л/с, ОФВ1 – от 7,5 до 8,8 л/с. У женщин: МОС вдоха – от 4,5 до 6,7 л/с, ОФВ1 – от 4,5 до 8,5 л/с. Спортсмены показали значения свыше 10,0 л/с по обоим показателям. Полученные данные систематизированы по половому признаку и использованы в качестве референсных интервалов для тренажёра[32].

Нормативные границы тренажёра дифференцированы по категориям: мужчины (МОС вдоха: 4,7–7,0 л/с, ОФВ1: 4,3–6,4 л/с), женщины (МОС вдоха: 3,5–5,0 л/с, ОФВ1: 3,3–4,2 л/с), спортсмены (более 10,0 л/с). Референсные интервалы верифицированы на основе учебно-методических пособий по исследованию функции внешнего дыхания.

Архитектура программного модуля: «LEARN PHYSIOLAB» включает пять тренажёров, каждый отвечает за свою диагностическую процедуру или лабораторный эксперимент. Все они собраны в общее меню. Параметры пациента каждый раз генерируются заново – это исключает механическое заучивание ответов и заставляет студента вдумываться.

В тренажёре АВ0 и резус-фактора для каждого студента генерируется случайный пациент. Студент выбирает метод – цоликлоны, сыворотки или эритроциты, – вносит реагенты в лунки и по анимированным частицам смотрит, произошла ли агглютинация. В тренажёре гемостаза даётся клинический сценарий травмы, нужно определить тип кровотечения и восстановить последовательность свёртывания крови. Всего восемь сценариев, один из них – с нарушением коагуляции при гемофилии[33].

В тренажёре пикфлоуметрии программа выбирает случайный тип пациента – ребёнок, женщина, мужчина, спортсмен или беременная, – и подставляет его норму ПСВ. Студент расставляет границы зон: красная (до 50 % нормы), жёлтая (50–80 %), зелёная (выше 80 %). Затем выполняет виртуальный выдох и смотрит, в какую зону попал результат. Проверка двухэтапная: сначала оценивается расстановка маркеров, потом – правильность определения зоны. Нормы ПСВ привязаны к возрасту и полу пациента[34, 35].

---

[30] Физиология человека : учебник / под ред. В. М. Покровского, Г. Ф. Коротько. 2-е изд., перераб. и доп. М. : Медицина, 2003. С. 656.

[31] Анохин М. Указ. соч. С. 104.

[32] Ольховская Е. А., Соловьева Е. В., Шкарин В. В. Исследование функции внешнего дыхания : учеб.-метод. пособие. 7-е изд. Н. Новгород : Издательство ПИМУ (НижГМА), 2018. С. 60.

[33] Гемофилия : учеб. электрон. пособие для обучающихся по направлениям подготовки специалитета «Педиатрия» и «Лечебное дело» / М-во науки и высш. образования Рос. Федерации, Федер. гос. бюджет. образоват. учреждение высш. образования Петрозав. гос. ун-т ; авт.-сост. М. С. Светлова. Петрозаводск : Издательство ПетрГУ, 2023. С. 36.

[34] Сапарова Л. Т. Мониторинг пиковой скорости выдоха у детей больных бронхиальной астмой : учебное пособие. Астана : [б. и.], 2007. С. 36.

[35] Черкашин Д. В., Шарова Н. В., Захарова И. М. Пикфлоуметрия при бронхиальной астме : учебное пособие. СПб. : Политехника, 2015. С. 71.

Технически сложнее всего устроен тренажёр пневмотахометрии. Он включает графическую модель манометра с двойной шкалой (внутренняя – для отсчёта в л/с, внешняя – для детализации), подвижную стрелку, анимированные лёгкие, расширяющиеся и сужающиеся при дыхании, а также переключаемую трубку для смены режимов (вдох/выдох). Студент выбирает пол пациента, задаёт режим, поворачивает трубку так, чтобы метка совпала с выбранным режимом, и, удерживая кнопку, имитирует дыхательное усилие. Стрелка движется в реальном времени, при отпускании кнопки результат фиксируется. Алгоритм check_results сверяет введённые показатели с нормативами и выдаёт заключение: норма, рестрикция, обструкция или смешанное нарушение[36].

Тренажёр питуитрина и меланофоров основан на классическом физиологическом опыте. Сначала студент делает гипофизэктомию, затем вводит питуитрин и смотрит, как меняется окраска кожи лягушки. Виртуальный микроскоп показывает, что происходит с меланофорами: пигмент меланина то собирается, то расходится по клетке. Так наглядно изучаются механизмы гормональной регуляции.

Шкала пневмотахометра сделана нелинейной. Для вдоха она содержит 10 опорных точек – от 0 до 9 л/с, с углами от 270° до −60°. Внешняя шкала детализации разбита на 13 точек (0–1,8 л/с с шагом 0,1–0,2 л/с). Числовое значение переводится в угол отклонения стрелки через кусочно-линейную интерполяцию: функция value_to_angle находит нужный интервал между опорными точками и вычисляет угол. Обратная функция angle_to_value по углу восстанавливает показание. Если значение превышает 9 л/с, срабатывает механизм пересчёта с учётом полных оборотов стрелки – каждые 10 л/с дают один полный оборот.

Асинхронная функция breathe_loop обновляет положение стрелки с частотой около 30 кадров в секунду, что создаёт эффект плавного движения. Скорость движения стрелки определяется функцией generate_speed: для выбранного пола и режима из статистической выборки случайным образом выбирается пара (пиковое значение, время достижения пика), на основе которой вычисляется угловая скорость в градусах в секунду. Коэффициент замедления 0,85 обеспечивает реалистичное время выполнения дыхательного маневра.

Визуализация лёгких реализована через группу контейнеров, изменяющих ширину, высоту и положение в зависимости от текущего значения объёмной скорости. При вдохе лёгкие расширяются, при выдохе – сужаются. Цветовая индикация меняется: левое лёгкое отображается розовым оттенком, правое – более тёмным, что имитирует разницу в анатомической форме и вентиляции. Трахея и бронхи также изменяют геометрию синхронно с дыхательным циклом.

Программные проверки безопасности блокируют переключение режимов при активном дыхании и предупреждают о несовпадении маркировки трубки с выбранным режимом. Алгоритм верификации (check_results) принимает введённые студентом значения МОС вдоха и ОФВ1, сравнивает их с эталонными показаниями прибора (допуск 4 %) и нормативами для выбранного пола. По результатам выдаётся одно из четырёх диагностических заключений.

Разработанный модуль реализует образовательный принцип «изучил – применил – закрепил»: каждый тренажёр содержит встроенный теоретический блок, доступный без переключения между приложениями. Система случайной генерации пациентов полностью исключает возможность запоминания ответов, вынуждая студента каждый раз проводить самостоятельный анализ. Методология построения заданий соответствует принципам, изложенным в практикуме по нормальной физиологии для студентов второго курса лечебного факультета. В тренажёре определения групп крови, например, случайным образом выбирается группа (0, A, B, AB), резус-фактор и интенсивность реакции, что даёт 16 возможных комбинаций, каждая с уникальной картиной агглютинации.

В отличие от коммерческих симуляторов спирографии и других диагностических процедур, стоимость которых зачастую высока для вузовского бюджета, предлагаемое решение является бесплатным, расширяемым и покрывает пять разделов физиологии. Встроенная теоретическая база содержит справочный материал по каждому разделу: механизмы агглютинации, каскад свёртывания, нормы ПСВ, физиологию дыхания[37].

В основу нормативной базы тренажёра положены действующие клинические рекомендации по интерпретации спирографических данных и диагностике нарушений бронхиальной проходимости[38].

---

[36] Собченко С. А. Пикфлоуметрия в лечении бронхиальной астмы / С. А. Собченко, О. С. Счетчикова, Е. В. Лешенкова, С. Н. Поспелова // В помощь практическому врачу. 2010. С. 775.

[37] Тулегенова Л. М. Использование пикфлоуметрии для скрининга и мониторирования бронхиальной проводимости : учеб.-метод. пособие. МинЗдрав РК, Западно-Казахстанская ГМА им. М. Оспанова. Актобе : [б. и.], 2008. С. 33.

[38] Рубан А. П., Сушинский В. Э., Маничев И. А. Диагностика нарушений бронхиальной проходимости и оценка контроля бронхиальной астмы : учеб.-метод. пособие. Минск : БГМУ, 2024. С. 32.

Параметры цветовых зон пикфлоуметрии соответствуют международным стандартам: зелёная зона – ПСВ более 80 % от должного значения, жёлтая – 50–80 %, красная – менее 50 %[39].

Апробация среди студентов медицинских специальностей показала, что работа с программой способствует формированию алгоритмического подхода к диагностике, а также снижает количество ошибок при последующей работе с реальным оборудованием. Отмечено, что наличие визуальной обратной связи (анимация лёгких, движение стрелки, цветовая индикация зон) улучшает понимание физиологических процессов.

В ходе исследования разработан и программно реализован модуль «LEARN PHYSIOLAB», объединяющий пять тренажёров по физиологии. Математическая модель пневмотахометрии построена на основе натурных измерений функции внешнего дыхания у 20 студентов Ижевского государственного медицинского университета, что обеспечивает адекватность и клиническую достоверность симулируемых данных.

Применение языка Python и фреймворка Flet позволило создать кроссплатформенное приложение, не требующее установки дополнительного программного обеспечения, что упрощает его внедрение в учебный процесс. Модуль может быть интегрирован в практическую подготовку студентов медицинских вузов как дополнение к существующим лабораторным занятиям.

Направления дальнейшего развития включают расширение набора тренажёров на другие разделы физиологии, внедрение автоматической системы оценки знаний с ведением статистики успеваемости, а также интеграцию с LMS-платформами для дистанционного обучения.

УДК 004.056:004.773.3(045)

Д. А. Васильченко, М. А. Фролов,
обучающиеся 4 курса Института права,
социального управления и безопасности ФГБОУ ВО «УдГУ».
Научный руководитель: Т. Н. Стерхова, канд. техн. наук, доцент
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Разработка приложения AntiPhish AI, предназначенного для защиты электронной почты от фишинга, на основе машинного обучения

Электронная почта остаётся одним из основных каналов деловой и личной коммуникации: её ежедневно используют около 60% населения Земли, а ежемесячный объём исходящей корреспонденции только в России превышает 625 млн писем. Высокая востребованность сервиса делает его привлекательной площадкой для злоумышленников. Отраслевая статистика подтверждает, что более 80 % инцидентов информационной безопасности в организациях инициируются через фишинговые письма.

Традиционные антивирусные решения и почтовые фильтры, опирающиеся на статические правила, чёрные списки и сигнатурный анализ, зачастую не способны своевременно идентифицировать zero-day угрозы и таргетированные атаки. Критическим уязвимым звеном остаётся человеческий фактор: даже подготовленные пользователи подвержены когнитивным искажениям, спешке и доверию к визуально знакомым интерфейсам.

Целью работы является разработка приложения AntiPhish AI, сочетающего традиционные методы фильтрации с алгоритмами машинного обучения для автоматического анализа безопасности электронных сообщений и повышения эффективности обнаружения фишинга в реальном времени. В рамках исследования были решены следующие задачи: анализ современных схем фишинга и методов маскировки; разработка алгоритма извлечения контекстно-поведенческих признаков; подготовка и интеграция гибридной ML-модели; создание десктопного приложения с графическим интерфейсом; экспериментальная оценка метрик качества и сравнение с коммерческими аналогами.

Современный фишинг эволюционировал из массовых рассылок в фоновый, автоматизированный и легко масштабируемый процесс. К наиболее актуальным векторам атак относятся:

1. BEC-атаки (Business Email Compromise) – имитация переписки от руководства, юридических отделов или контрагентов.

[39] Сапарова Л. Т. Указ. соч. С. 36.

2. Кража учётных данных – массовые рассылки с ссылками на фальшивые страницы авторизации банков, государственных порталов и корпоративных систем.

3. QR-фишинг (Quishing) – внедрение вредоносных QR-кодов непосредственно в тело письма, что усложняет автоматическую проверку ссылок.

4. AI-усиленный таргетированный фишинг – использование больших языковых моделей для генерации персонализированных, стилистически корректных сообщений[40].

Для обхода средств фильтрации злоумышленники применяют комплексные техники маскировки: доменный и визуальный спуфинг (регистрация оптически схожих доменов, клонирование HTML-шаблонов), обход проверок SPF/DKIM/DMARC через скомпрометированные легитимные учётные записи, техническую обфускацию контента (макросы, динамическая подгрузка форм, кодирование URL, использование легитимных сокращателей) и социально-инженерное давление (создание искусственной срочности, угрозы блокировки). В данных условиях требуется решение, сочетающее эвристический анализ, поведенческое детектирование и репутационную оценку внешних объектов.

Алгоритм извлечения признаков реализован как многоуровневая аналитическая система, ориентированная на выявление как статических, так и контекстно-поведенческих маркеров угрозы.

1. Репутационная фильтрация. На начальном этапе инфраструктурные атрибуты отправителя сверяются с агрегированными белыми и чёрными списками, включающими проверенные домены и исторические данные о рассылках. Это позволяет блокировать известные угрозы на этапе подключения и снижать нагрузку на последующие модули.

2. Нейросетевой анализ контента. Модуль обработки естественного языка анализирует тему, тело письма и метаданные, извлекая поведенческие признаки: манипулятивные речевые паттерны, грамматические аномалии, искусственную срочность. Контекстные маркеры формируются на основе тональности сообщения, частотности триггерных конструкций («срочно подтвердите», «обновите реквизиты», «аккаунт будет заблокирован») и отклонений от типичных рабочих сценариев адресата.

3. Внешняя верификация через VirusTotal API. Все извлечённые URL и вложения передаются на сканирование. Сервис агрегирует данные десятков антивирусных движков, возвращая хеши файлов, статусы доменов, историю редиректов и репутационные оценки, что обогащает контекст письма для финального расчёта риска.

4. Система принятия решений. Совокупность признаков нормируется, взвешивается по значимости и подаётся на классификатор, формирующий итоговую оценку безопасности. Такой подход позволяет нейтрализовать угрозы даже при отсутствии известных сигнатур[41].

В проекте реализован многоуровневый ИИ-конвейер, сочетающий готовые предобученные решения и специализированные собственные разработки:

- Базовый классификатор. Используется модель NebalAKKI/spam-email-classifier, размещённая на платформе openroute.ai. Выбор обусловлен высокой точностью на задачах бинарной классификации «спам/не спам» и оптимизацией для работы в реальном времени через API, что исключает необходимость развёртывания тяжёлых вычислительных ресурсов на стороне клиента.
- Собственные детекторы. Параллельно работают две кастомные модели:

1) детектор текста, сгенерированного ИИ, анализирующий стилистические и статистические особенности сообщений;

2) детектор паттернов неотложных действий (urgency patterns), обучаемый распознавать лингвистические конструкции, создающие искусственное давление на получателя.

Модели работают последовательно в едином аналитическом контуре, обеспечивая устойчивость как к массовым рассылкам, так и к сложным таргетированным атакам[42].

Приложение AntiPhish AI реализовано на языке Python с использованием библиотеки CustomTkinter и функционирует как самостоятельный десктопный клиент. Архитектура включает два основных окна:

- Окно авторизации обеспечивает безопасное подключение к почтовому ящику по протоколу IMAP.

---

[40] Кутергин Д. С. Информационная безопасность пользователей электронной почты // LII итоговая студенческая научная конференция Удмуртского государственного университета : материалы Всерос. конф., Ижевск, 23–25 апреля 2024 года. Ижевск : Удм. гос. ун-т, 2024. С. 119–122.

[41] Стерхова Т. Н., Васильчекно Д. А. Рекомендации пользователям электронной почты по защите данных // Актуальные проблемы энергетики АПК : материалы III Национальной науч.-практ. конф. с междунар. участием им. Г. П. Ерошенко, Саратов, 18 апреля 2025 г. Саратов : Саратов. гос. ун-т генетики, биотехнологии и инженерии им. Н. И. Вавилова, 2025. С. 382–385.

[42] Стерхова Т. Н., Васильчекно Д. А. Основные угрозы и методы защиты информации пользователей электронной почты // Менеджмент безопасности жизнедеятельности: перспективы развития и проблемы преподавания : сб. материалов VI открытой Республиканской науч.-практ. интернет-конф., Минск, 12 декабря 2024 года. Минск : Ун-т гражд. защиты Министерства по чрезвычайным ситуациям Республики Беларусь, 2025. С. 115–117.

- Панель мониторинга содержит индикатор состояния защиты, блок статистики, интерактивную таблицу выявленных угроз, а также элементы управления (приостановка проверки, настройки, поддержка).

При выборе подозрительного письма в таблице открывается диалоговое окно с детализацией вердикта: оценка нейросетевого классификатора, выявленные паттерны социальной инженерии, результаты сканирования через VirusTotal и анализ заголовков на предмет спуфинга. Прозрачность работы системы выполняет не только защитную, но и образовательную функцию, способствуя повышению цифровой грамотности пользователей.

Эффективность системы оценивалась на смешанной выборке легитимных и вредоносных писем. Получены следующие метрики качества:

- точность детектирования – 86 %;
- доля ложноположительных срабатываний (FP) – 7 %;
- доля ложноотрицательных результатов (FN) – 7 %;
- скорость проверки одного письма – 5–12 секунд.

Скоростные показатели зависят от качества интернет-соединения, что обусловлено архитектурой, предполагающей множественные внешние запросы по API. Для объективной оценки конкурентоспособности проведено сравнение с коммерческими продуктами (см. табл. 1):

Таблица 1.

Сравнительная таблица приложения AntiPhish AI с аналогами

Программный продукт	Точность	Скорость
AntiPhish AI	86 %	5–12 секунд
Kaspersky Security Mail Gateway (KSMG)	96,8 %	1,5–3,2 секунды
Dr.Web Mail Server	94,6 %	1,8–3,6 секунды

Отставание в скорости объясняется различиями в архитектуре: корпоративные шлюзы оперируют локальными сигнатурными базами и выделенными серверными ресурсами, тогда как AntiPhish AI выполняет кроссплатформенные API-запросы в реальном времени. Однако, ключевое преимущество разработанного решения заключается в отсутствии требований к серверной инфраструктуре и операционной системе Linux, что устраняет необходимость в выделенном оборудовании и сложной настройке.

В ходе работы достигнута поставленная цель: создано десктопное приложение AntiPhish AI, объединяющее традиционные методы фильтрации с гибридной моделью машинного обучения для защиты электронной почты в реальном времени. Разработанное решение корректно идентифицирует 86 % вредоносных писем, обеспечивает прозрачность вердиктов для пользователя и не требует развёртывания серверной инфраструктуры. Продукт заполняет значимую нишу между базовыми встроенными фильтрами почтовых провайдеров и дорогостоящими enterprise-системами, делая продвинутую защиту доступной для малого бизнеса, индивидуальных предпринимателей и частных пользователей.

Дальнейшее развитие системы будет направлено на:

1. Расширение обучающей выборки для повышения точности классификации.
2. Оптимизацию скорости работы за счёт кэширования результатов проверок и асинхронной обработки запросов.
3. Интеграцию поддержки дополнительных почтовых протоколов.
4. Разработку серверной версии продукта для корпоративного сегмента.

Реализованный подход демонстрирует, что эффективная защита от фишинга может быть обеспечена за счёт комбинации репутационного анализа, нейросетевой обработки естественного языка и внешней верификации объектов, что открывает перспективы для масштабирования технологии в условиях растущего использования ИИ злоумышленниками.

УДК 343.13:004(045)

Д. А. Вольхин,
обучающийся 3 курса Института права,
социального управления и безопасности ФГБОУ ВО «УдГУ».
Научный руководитель: Ф. А. Абашева, канд. юрид. наук, доцент
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Информационное обеспечение судебного порядка получения разрешения на производство следственных действий

В процессе осуществления предварительного расследования нередко возникают ситуации, когда в целях более точного и быстрого раскрытия преступления необходимо оперативное совершение определенных следственных действий. Эти следственные действия, в силу того, что ограничивают в той или иной мере конституционные права граждан, должны получить судебное разрешение. У следователя или дознавателя как непосредственных субъектов расследования по мере раскрытия преступления, взаимодействия с элементами преступления (вещественными доказательствами, потерпевшим, свидетелями и т. д.) складывается определенное понимание произошедшего события. Судья, рассматривая ходатайство следователя или дознавателя, не имеет того понимания, которое сложилось у последних; судья лишь опосредствовано узнает об обстоятельствах произошедшего. Вследствие, судье трудно определить, являются ли доводы, приведенные следователем или дознавателем в ходатайстве, достаточно обоснованными для получения разрешения на производство следственных действий.

Таким образом, существует проблема в передаче информации о предполагаемом преступлении от непосредственного субъекта расследования (следователя или дознавателя) к судье.

Статья имеет своей целью анализ информационного обеспечения процедуры судебного порядка получения разрешения на производство следственных действий, выявление проблем данного обеспечения и формулирование путей их решения.

Исследование информационного обеспечения судебного порядка получения разрешения на производство следственных действий необходимо начать с раскрытия ключевых понятий, используемых в данной работе. Для начала нужно определить, что такое информационно обеспечение. В уголовно-процессуальном законодательстве не содержится прямое определение понятия «информационное обеспечение» применительно к рассматриваемой нами процедуре. Однако ряд норм УПК РФ[43] позволяет косвенным путем сформулировать определение.

Первая и главная норма содержится в ст. 165 УПК РФ. Данная статья устанавливает порядок рассмотрения ходатайства следователя или дознавателя о производстве следственных действий, требующих судебного решения. Положения статьи указывают на необходимость представления материалов, обосновывающих ходатайство. Статья 182 УПК РФ требует наличия достаточных данных для проведения обыска. Статья 184 УПК РФ указывает на необходимость оснований для производства личного обыска подозреваемого, обвиняемого. Статья 185 УПК РФ требует наличия достаточных оснований для наложения ареста на почтово-телеграфные отправления, их осмотр и выемку. Статья 186 УПК РФ обязывает указывать в ходатайстве о производстве контроля и записи телефонных и иных переговоров основания для проведения данного следственного действия.

В научной литературе существует множество определений понятия «информационное обеспечение», которое дается применительно к конкретной задаче исследования. Например, А. М. Ишин дает такое определение понятия «информационное обеспечение»: « …информационное обеспечение – это совокупность единой системы сбора и получения информации из внешних и внутренних источников, схем информационных потоков, циркулирующих в ходе раскрытия и расследования преступлений, а также методология использования имеющихся баз данных и построения новых баз данных»[44].

Для задач данной статьи, исходя из вышеизложенного, можно сформулировать следующее определение понятия «информационное обеспечение» применительно к судебному порядку получе-

[43] Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (ред. от 09.04.2026) // СЗ РФ. 2001. № 52 (ч. I). Ст. 4921.

[44] Ишин А. М. Информационное обеспечение предварительного расследования преступлений: некоторые современные аспекты // Вестник БФУ им. И. Канта. 2016. № 4. С. 21–28. URL: https://cyberleninka.ru/article/n/informatsionnoe-obespechenie-predvaritelnogo-rassledovaniya-prestupleniy-nekotorye-sovremennye-aspekty/viewer (дата обращения: 04.05.2026).

ния разрешения на производство следственного действия: информационное обеспечение – это совокупность сведений и документов, которые следователь (дознаватель) обязан представить суду для обоснования ходатайства о производстве следственного действия.

Уголовно-процессуальный кодекс РФ не содержит четкого определения следственных действий; главы 24–27 УПК РФ закрепляют лишь перечень и порядок производства следственных действий. Из норм закона можно выделить ключевые признаки следственных действий: 1) регламентированность уголовно-процессуальным законом; 2) направленность на сбор доказательств; 3) обязательность фиксации результатов. Доктрина предлагает нам развернутые определения. С. А. Шейфер характеризует следственные действия как «регламентированные уголовно-процессуальным законом действия, посредством которых органы расследования и суд обнаруживают, закрепляют, проверяют и оценивают доказательства»[45]. В. А. Семенцов подчеркивает их познавательную и удостоверяющую функции, определяя следственные действия как способы получения информации о событии преступления и лицах, его совершивших[46].

Статья 165 УПК РФ регламентирует процедуру подачи и рассмотрения ходатайства о производстве следственных действий, требующих судебного разрешения. Закон устанавливает: письменную форму ходатайства; его содержание (основания, мотивы, данные о лице); срок рассмотрения. Доктрина дополняет эти положения, выделяя критерии качества ходатайства. О. В. Химичева отмечает, что оно должно содержать: ссылку на норму УПК РФ; фактические обстоятельства, обосновывающие необходимость действия; перечень прилагаемых материалов[47]. Л. Н. Масленникова обращает внимание на стандартах доказывания: ходатайство должно исключать сомнения в необходимости проведения следственного действия[48].

Таким образом, еще при установлении определений и раскрытии основных понятий мы наталкиваемся на ряд проблем: 1) отсутствие четких определений ключевых понятий, что создает трудности в правоприменении, в частности при оценке достаточности оснований для производства следственных действий; нормативные положения не всегда учитывают современные вызовы, такие как работа с электронными доказательствами.

Следующим шагом мы должны рассмотреть этапы получения разрешения на производство следственного действия и выявить важны для задач данного исследования моменты.

Первый этап получения разрешения на производство следственного действия заключается в установлении следователем (дознавателем) оснований для производства данного действия.

Как отмечается в научной литературе, существует два вида оснований для производства следственных действий: 1) фактическое основание; 2) правовое основание[49]. Фактическое основание составляют сведения, полученные следователем или дознавателем как непосредственными субъектами расследования, которые указывают на необходимость производства следственного действия. Правовое основание составляют те нормы уголовно-процессуального законодательства, которые регламентируют порядок производства нужного следственного действия (например, ст. 182, 186 УПК РФ и т. д.).

Рассматривая процесс расследования с точки зрения наличия двух видов оснований для производства следственного действия можно заметить, что проблемным моментом является фактическое основание, поскольку именно оно подвержено субъективной оценке.

Следующим этапом является составление следователем (дознавателем) ходатайства о производстве необходимого следственного действия и рассмотрение данного ходатайства судом[50]. Выделим несколько моментов в данном этапе.

Первым моментом является подготовка ходатайства. В этом моменте представляет интерес для нашего исследования деятельность следователя (дознавателя) по собиранию и систематизации материалов, подтверждающих необходимость следственного действия. Согласно п. 1 ПП ВС РФ от 01.06.2017 № 19, судья должен выяснить приложены ли к ходатайству: копии постановлений о возбуждении уголовного дела и принятии уголовного дела к производству, о продлении срока

---

[45] Шейфер С. А. Следственные действия. Система и процессуальная форма. М. : Юрлитинформ, 2001. С. 25.

[46] Семенцов В. А. Следственные действия : учебное пособие. Екатеринбург : УрГЮА, 2003. С. 12.

[47] Химичева О. В. Досудебное производство по уголовным делам: концепция совершенствования уголовно процессуальной деятельности. М. : Экзамен, 2003. С. 112.

[48] Масленникова Л. Н. Методология познания уголовно-процессуального права. М. : Юстиция, 2018. С. 67.

[49] Фактические и правовые основания производства следственных действий // КиберЛенинка. URL: https://cyberleninka.ru/article/n/fakticheskie-i-pravovye-osnovaniya-proizvodstva-sledstvennyh-deystviy/viewer (дата обращения: 04.05.2026).

[50] Производство следственных действий по решению суда // КиберЛенинка. URL: https://cyberleninka.ru/article/n/proizvodstvo-sledstvennyh-deystviy-po-resheniyu-suda/viewer (дата обращения: 04.05.2026).

предварительного расследования, о возобновлении производства по уголовному делу, материалы, подтверждающие наличие оснований для производства следственного действия, и др.[51].

Вторым интересующем нас моментом является рассмотрение ходатайства судом. Суд изучает представленные материалы и оценивает законность, обоснованность производства необходимого следственного действия[52].

Рассмотрев интересующие нас моменты получения судебного разрешения на производство следственного действия, мы можем сформулировать актуальные на сегодняшний день проблемы информационного обеспечения данной процедуры.

Уголовно-процессуальное законодательство не в полной мере отвечает запросам цифрового развития передачи информации. В уголовно-процессуальном законодательстве нет четкого регулирования порядка получения, фиксации и использования информации, хранящейся на электронных носителях или полученной с помощью телекоммуникационных сетей. В связи с этим создается трудность, например, при решении вопроса, требуется ли судебное решение для осмотра информации на электронном носителе в рамках осмотра места происшествия[53]. Отсутствуют правила и методы работы с электронными следами преступления. Данное обстоятельство может привести к невозможности получить ключевые данные, сведения, которые могут быть использованы в качестве доказательств в суде. Создается трудность для следователя (дознавателя) в отражении полученной информации в фактическом основании ходатайства.

Между правоохранительными органами и судами нет четкой электронной информационной связи, с помощью которой можно было бы передавать точные данные о расследовании преступления, в том виде, в каком ее зафиксировал следователь (дознаватель). Сюда же можно отнести низкий уровень подготовки сотрудников по работе с информационными технологиями. Создается трудность для более точного восприятия судьей тех сведений, которые были установлены следователем (дознавателем).

В результате данных обстоятельств сбор и систематизация доказательств наличия достаточных оснований для проведения определенного следственного действия осложняются из-за проблем с доступом к информации, ее качеством и формой представления.

В связи с этим для улучшения информационного обеспечения процедуры можно предложить такие меры, как:

1. Введение в уголовно-процессуальное законодательство положений в части регулирования работы с электронными доказательствами и информационными технологиями в уголовном процессе. Определить уровень подготовки сотрудников для работы с указанными технологиями, установить правила, методики по работе с электронными доказательствами. Это позволит точно, наиболее достоверно отразить в ходатайстве полученные следователем (дознавателем) сведения о преступлении.

2. Введение единой информационной системы для передачи информации между правоохранительными органами и судами. Это позволит более ясному и четкому восприятию судьями доказательств наличия достаточных оснований для проведения нужного следственного действия.

[51] О практике рассмотрения судами ходатайств о производстве следственных действий, связанных с ограничением конституционных прав граждан (статья 165 УПК РФ) : постановление Пленума Верховного Суда РФ от 01.06.2017 № 19 // Российская газета. 2017. № 125.

[52] Подготовка к рассмотрению ходатайства о производстве следственных действий в уголовно процессуальном праве Российской Федерации // КиберЛенинка. URL: https://cyberleninka.ru/article/n/podgotovka-k-rassmotreniyu-hodataystva-o-proizvodstve-sledstvennyh-deystviy-v-ugolovno-protsessualnom-prave-rossiyskoy-federatsii/viewer (дата обращения: 04.05.2026).

[53] Валитова В. И. Проблема применения «электронных» доказательств в уголовном процессе // Шаг в науку. 2025. № 3. С. 90–95. URL: https://cyberleninka.ru/article/n/problema-primeneniya-elektronnyh-dokazatelstv-v-ugolovnom-protsesse/viewer (дата обращения: 04.05.2026).

УДК 004.056.57:621.311(045)

А. А. Востриков,
обучающийся 4 курса Института права,
социального управления и безопасности ФГБОУ ВО «УдГУ».
Научный руководитель: Т. Н. Стерхова, канд. техн. наук, доцент
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Угрозы нулевого дня

Одной из наиболее опасных современных угроз являются угрозы нулевого дня (zero-day). Они связаны с использованием уязвимостей в программном обеспечении, о которых еще не известно разработчикам и специалистам по информационной безопасности. Это означает, что на момент атаки не существует готовых средств защиты, что значительно усложняет их обнаружение и предотвращение.

Актуальность темы обусловлена тем, что электроэнергетика относится к критической инфраструктуре. Любые сбои в ее работе могут привести к серьезным последствиям: от экономических потерь до нарушения нормальной жизнедеятельности населения. В условиях высокой автоматизации такие риски становятся особенно значимыми.

Целью данной работы является изучение угроз нулевого дня и способов защиты от них в электроэнергетике.

Угрозы нулевого дня (zero-day threats) относятся к числу наиболее сложных и труднообнаружимых киберугроз в современной практике обеспечения информационной безопасности. Под уязвимостью нулевого дня понимается ранее неизвестная разработчику программного обеспечения ошибка или дефект, который может быть использован злоумышленником для реализации несанкционированного доступа, выполнения произвольного кода или нарушения целостности и доступности системы.

Ключевой характеристикой zero-day уязвимостей является отсутствие сигнатур и патчей на момент их эксплуатации. В связи с этим традиционные средства защиты, основанные на сигнатурном анализе (антивирусные решения, классические IDS/IPS), оказываются недостаточно эффективными. Это обусловливает необходимость применения проактивных и поведенческих методов обнаружения угроз.

С точки зрения классификации, уязвимости нулевого дня могут относиться к различным категориям: ошибки управления памятью (например, переполнение буфера), уязвимости аутентификации и авторизации, логические ошибки в бизнес-процессах, а также уязвимости в сетевых протоколах и промышленных системах управления.

Жизненный цикл уязвимости нулевого дня включает несколько взаимосвязанных этапов. На первом этапе осуществляется обнаружение уязвимости, которое может происходить как в рамках легитимных исследований (в том числе программ bug bounty), так и в результате целенаправленного поиска злоумышленниками. Далее следует этап разработки эксплойта – программного инструмента, реализующего механизм использования уязвимости. На этапе эксплуатации уязвимость применяется для проведения атак, зачастую в рамках целевых кампаний (Advanced Persistent Threat, APT). После раскрытия информации об уязвимости начинается разработка и распространение патча, однако до момента его массового внедрения система остается уязвимой.

Одной из ключевых особенностей АСУ ТП является их изначальная ориентация на надежность и непрерывность технологических процессов, а не на кибербезопасность. Многие промышленные системы проектировались без учета современных угроз, что приводит к наличию устаревших протоколов связи, отсутствию механизмов шифрования и аутентификации, а также ограниченным возможностям обновления программного обеспечения. В таких условиях уязвимости нулевого дня становятся особенно опасными, поскольку их эксплуатация может длительное время оставаться незамеченной.

Угрозы нулевого дня в электроэнергетике[54] могут затрагивать различные уровни инфраструктуры: от корпоративных информационных систем до нижнего уровня управления оборудованием (контроллеры, датчики, исполнительные устройства). Наиболее критичными являются атаки, направленные на программируемые логические контроллеры (ПЛК) и серверы SCADA, поскольку их компрометация позволяет злоумышленнику непосредственно влиять на технологические процессы.

[54] Рудов А. В., Кушнир Д. В. Информационная безопасность электростанций // Аспект. URL: https://na-journal.ru/6-2022-informacionnye-tekhnologii/3989-informacionnaya-bezopasnost-electrostancii (дата обращения: 18.05.2026).

Сложность выявления угроз нулевого дня в электроэнергетике обусловлена рядом факторов. Во-первых, в промышленных сетях часто используются специализированные протоколы и оборудование, для которых отсутствуют эффективные средства анализа трафика. Во-вторых, внедрение обновлений и патчей может быть затруднено из-за необходимости обеспечения непрерывности технологических процессов. В-третьих, многие системы функционируют в условиях ограниченных вычислительных ресурсов, что затрудняет использование современных средств защиты.

Дополнительным фактором риска является интеграция производственных и корпоративных сетей (IT и OT-среды). Такая конвергенция повышает вероятность проникновения угроз из внешней среды во внутренние сегменты АСУ ТП. В этом контексте уязвимости нулевого дня могут использоваться как начальная точка атаки с последующим распространением по инфраструктуре.

Обеспечение защиты[55] от угроз нулевого дня представляет собой одну из наиболее сложных задач современной кибербезопасности, поскольку такие угрозы по определению не имеют известных сигнатур на момент атаки. В связи с этим классические методы защиты, основанные на сигнатурном анализе вредоносного кода, оказываются недостаточно эффективными. Это особенно критично для систем электроэнергетики и АСУ ТП[56], где требуется высокая надежность и непрерывность функционирования.

Кроме того, в промышленных сетях АСУ ТП часто ограничено использование ресурсоемких средств защиты, что дополнительно снижает эффективность классических решений.

Одним из ключевых направлений противодействия угрозам нулевого дня является использование поведенческого анализа (behavior-based detection) и методов выявления аномалий. Данный подход основан не на поиске известных сигнатур, а на анализе отклонений в поведении пользователей, приложений и сетевого трафика.

Методы машинного обучения[57] и статистического анализа позволяют формировать модель «нормального» функционирования системы, после чего любые отклонения рассматриваются как потенциально подозрительные. Такой подход особенно эффективен в автоматизированных системах управления технологическими процессами, где технологические процессы обычно характеризуются стабильностью и предсказуемостью.

Методы превентивной защиты включают меры, которые помогают предотвратить использование уязвимостей в системе безопасности еще до того, как они будут использованы злоумышленником. Обычно к таким методам относятся:

- Sandboxing (песочницы) – запуск потенциально опасных объектов в изолированной среде, чтобы изучить их действия без риска для системы;
- Обфускацию и ASLR – приемы, усложняющие успешную эксплуатацию ошибок, связанных с памятью, за счет сокрытия или случайного изменения адресов;
- RASP (Runtime Application Self-Protection) – механизм, который отслеживает работу приложения прямо во время выполнения и позволяет выявлять подозрительное поведение в реальном времени.
- Threat hunting – это превентивное выявление незаметных признаков возможных атак и подозрительной активности в ИТ-среде.

Использование таких методов помогает свести к минимуму риск успешной эксплуатации уязвимости, даже если о готовом способе устранения пока ничего не известно.

Для уменьшения последствий атак нулевого дня используется комплекс организационных и технических решений, ориентированных на быстрое обнаружение и локализацию угроз. Одним из основных элементов такой защиты является процесс реагирования на инциденты информационной безопасности: он охватывает обнаружение, изоляцию, устранение последствий и последующее восстановление нормальной работы систем.

Кроме того, для повышения уровня защиты внедрены инструменты непрерывного мониторинга, такие как SIEM-платформы. Они собирают и анализируют события безопасности в режиме реального времени, что помогает обнаруживать подозрительную активность и заранее распознавать возможные сценарии атак.

---

[55] Рыбаков С. Ю., Ташлыков Ф. А. Анализ подходов к обнаружению атак нулевого дня в сетях интернета вещей // Инженерный вестник Дона. 2025. № 7. URL: https://cyberleninka.ru/article/n/analiz-podhodov-k-obnaruzheniyu-atak-nulevogo-dnya-v-setyah-interneta-veschey/viewer (дата обращения: 18.05.2025).

[56] Петров Н. А. Целенаправленные атаки – обнаружение и защита. URL: https://www.dialognauka.ru/press-center/posts/articles/tselenapravlennye-ataki-obnaruzhenie-i-zashchita-2718/ (дата обращения: 18.05.2026).

[57] Дубровина А. И., Алкорди М. Х. Разработка методов нейтрализации угроз «нулевого дня» // Вестник Дагестанского государственного технического университета. Технические науки. 2023. Т. 50, № 4 // URL: https://cyberleninka.ru/article/n/razrabotka-metodov-neytralizatsii-ugroz-nulevogo-dnya/viewer (дата обращения: 18.05.2026).

Одним из наиболее перспективных направлений в кибербезопасности сегодня становится создание интеллектуальных механизмов, способных распознавать угрозы с помощью методов машинного обучения[58], искусственного интеллекта и глубоких нейросетевых моделей. Их главное преимущество заключается в возможности анализировать большие объемы информации, находить неясные зависимости и, соответственно, обнаруживать новые сценарии атак, которые ранее не были обнаружены.

Помимо этого, все больше внимания уделяется применению цифровых двойников (Digital Twin), которые позволяют воспроизводить работу промышленных объектов в виртуальной среде. За счет такого моделирования можно своевременно замечать аномалии в поведении систем и определять признаки кибервоздействий, влияющих на их работу.

В условиях растущего числа сложных угроз становится очевидно, что привычные механизмы защиты уже не дают требуемой эффективности. Поэтому на первый план выходят инструменты, позволяющие отслеживать подозрительное поведение, фиксировать отклонения от нормы и непрерывно анализировать события безопасности. Все более важными становятся и упреждающие меры – от sandboxing до threat hunting. Отдельно стоит отметить интеллектуальные системы, использующие машинное обучение и обработку больших массивов данных для выявления атак.

Эффективно снизить риски, связанные с атаками нулевого дня в энергетической отрасли, удаётся лишь при одновременном применении как технологических, так и управленческих решений. В их число входят разделение сетевой инфраструктуры на сегменты, использование актуальных средств контроля и анализа, укрепление защищённости АСУ ТП, а также создание особых механизмов быстрого реагирования на инциденты в сфере информационной безопасности.

УДК 004.738.5:[37+004.056](045)

Д. Р. Гареева,
обучающаяся 3 курса Нефтекамского филиала
ФГБОУ ВО «Уфимский университет науки и технологий».
Научный руководитель: А. Р. Аюпова, канд. физ.-мат. наук, доцент
Нефтекамского филиала ФГБОУ ВО «Уфимский университет науки и технологий»,
г. Нефтекамск

Использование VPN в образовательном процессе: безопасность и доступность ресурсов

Вследствие цифровой эволюции образовательной сферы, получившей мощный импульс в период пандемии и при дальнейшем становлении смешанных моделей учебы, электронные ведомости, платформы управления обучением (LMS), облачные репозитории методического контента и сервисы видеосвязи превратились в рутинный элемент функционирования школ, ссузов и вузов. В сложившихся обстоятельствах информационные потоки учебных заведений включают личные сведения учащихся и педагогического состава (фамильно-именные данные, локации проживания, контактные телефоны, показатели академической успеваемости), итоги научных изысканий, внутреннюю корреспонденцию, а также информацию, относимую к категории коммерческой либо должностной тайны. Трансляция означенных сведений по публичным каналам, в особенности при выходе в Сеть через публичные хот-споты Wi-Fi (заведения общепита, гибкие рабочие пространства, кампусные общежития), порождает существенные угрозы перехвата, искажения и несанкционированной утечки информации. Посредством технологии VPN (Virtual Private Network) организуется криптографически защищенный канал между клиентским оборудованием и интранетом образовательной организации, гарантируя приватность, неискажаемость и верификацию транслируемой информации. Тем не менее имплементация VPN в академическую практику связана не лишь с инженерными аспектами, но и с административно-юридическими трудностями, чем и продиктована злободневность данной работы[59].

[58] Аманова Ай., Мыратлыев Д., Урусдамов А. Применение алгоритмов машинного обучения для повышения эффективности систем обнаружения вторжений // Вестник науки. 2025. Т. 2, № 5 (86). URL: https://cyberleninka.ru/article/n/primenenie-algoritmov-mashinnogo-obucheniya-dlya-povysheniya-effektivnosti-sistem-obnaruzheniya-vtorzheniy/viewer (дата обращения: 18.05.2025).

[59] Гамзин Д. М., Тибалов Н. П., Поначугин А. В. Актуальность использования VPN-сервисов в России в условиях мировой нестабильности // Международный научно-исследовательский журнал. 2023. Т. 2, № 128. С. 25–30.

Исходя из характера связи, выделяют два фундаментальных типа VPN. К первому относится remote access VPN, нацеленный на персональное дистанционное подсоединение сотрудников к внутрикорпоративной либо вузовской сети. Для образовательной отрасли данная разновидность наиболее востребована, ибо позволяет каждому обучающемуся или лектору стыковаться с локальными мощностями, задействуя фирменное ПО клиента или нативные инструменты ОС. К примеру, вуз способен предоставить студентам пропуск к лицензируемым цифровым библиотекам исключительно по факту активации VPN-сессии с применением идентификационных реквизитов учащегося. Второй тип – site-to-site VPN – задействуется для сопряжения двух и более сегментов локальной сети, скажем, кампусов, периферийных отделений или учреждений-партнеров. При подобном раскладе межсетевой обмен шифруется и курсирует по интернету как целостный оберегаемый канал. Для академической среды указанный метод важен при консолидации информационных инфраструктур разрозненных площадок, реализации кооперированных программ межвузовского уровня или подсоединении обособленных учебных строений без прокладки физических оптических магистралей.

С позиции методологии формирования виртуального тоннеля дифференцируют продукты сетевого звена (IPsec) и средства, работающие на транспортном либо прикладном уровнях (SSL/TLS VPN). Для учебных институций критически важно, чтобы параметры VPN не порождали избыточных затруднений у конечного потребителя, так как чересчур мудреная настройка ведет к отторжению части аудитории от использования средств удаленной учебы. Посему зачастую предпочтение отдают SSL/TLS VPN, дающим возможность авторизации через стандартный браузер либо нетребовательный к ресурсам клиент. Надлежит также отличать ведомственный VPN, выделяемый учреждением, и публичные клиентские VPN-сервисы. Первые сориентированы на оберегаемый доступ к конкретным интранет-ресурсам и администрируются IT-департаментом вуза, вторые же чаще употребляются для преодоления гео-фильтров или оберегания приватного веб-серфинга. В академическом поле обе разновидности могут иметь хождение, однако ведомственный VPN гарантирует институциональный надзор и соблюдение регламентов инфобезопасности, в то время как клиентские сервисы подпадают под юрисдикцию посторонних фирм и способны привнести добавочные опасности[60].

Помимо указанного, VPN обеспечивает оборону удаленного системного управления. IT-специалисты и сисадмины могут получать доступ к серверному оборудованию LMS, базам данных учащихся, системам визуального контроля и иным значимым узлам только сквозь аутентифицированное VPN-соединение. Такой подход блокирует прямой вызов управленческих консолей из глобального интернета и кардинально понижает риск атак, сопряженных с брутфорсом либо уязвимостями веб-интерфейсов. Наконец, VPN благоприятствует становлению привычек цифровой осмотрительности в среде участников учебного процесса. Если для входа в среду дистанционного образования нужна активация VPN, это перманентно сигнализирует юзерам о надобности оберегаемого подключения и понижает шансы легкомысленного обращения (например отправки паролей незащищенными путями)[61].

Нормативно-правовое регулирование использования VPN в РФ. Задействование VPN в учебных институциях обязано производиться в жестком соответствии с отечественными законами. Основополагающим актом служит Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», вменяющий в обязанность владельцам информсистем внедрение организационно-технических механизмов ограждения данных при их трансфере по каналам общего доступа. Ключевую роль играет также Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», предписывающий операторам (а учреждение образования таковым для учащихся и персонала и является) гарантировать приватность и неуязвимость подобной информации в ходе ее процессинга, в том числе при перемещении по общедоступным сетям. Применение VPN с шифрованием канала расценивается надзорными ведомствами в качестве допустимого инструмента реализации данного императива, наравне с внедрением криптошлюзов и оберегаемых протоколов обмена[62].

При всем том следует разграничивать внутрикорпоративный VPN, администрируемый непосредственно учебным заведением, и общедоступные провайдерские VPN-службы. Образовательная институция, развертывая свою серверную часть VPN, тотально регулирует криптографию, журналирование и полномочия, что согласуется с нормами о локализации личных данных (ст. 18 Закона

[60] Белоусова М., Здоровец С., Алехина А. О правовых аспектах использования информационных технологий в процессе обучения // Цифровые технологии и право. 2023. Т. 1, № 1. С. 127–131.

[61] Федорова Я. Е., Чухнёв Д. А. Использование облачных ресурсов и цифровых платформ в образовательном процессе вуза // Педагогическое образование. 2023. Т. 4, № 9. С. 6–13.

[62] Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 28.12.2024) // СПС «КонсультантПлюс» (дата обращения: 10.04.2026).

№ 152-ФЗ). Эксплуатация же внешних, в особенности иностранных VPN-сервисов, чревата ситуацией, когда личные сведения обучающихся окажутся у посторонних лиц без должной законной аргументации. Более того, в силу ч. 1.1 ст. 15.2 Закона № 149-ФЗ, эксплуатация VPN с целью обхода реестров запрещенных веб-ресурсов, нахождение к которым на территории РФ ограничено, способна трактоваться как противоправное действие. Ввиду этого в локальных документах учебной организации надлежит ясно прописать легитимные основания для обращения к VPN (связь с интранет-мощностями, оборона информации, деятельность с лицензируемыми БД) и воспретить его использование для обхода законодательных табу[63].

Опыт тотальной миграции на удаленный режим занятий в 2020–2021 гг. обнажил и набор стандартных затруднений. Самыми массовыми оказались перегруз пропускных мощностей каналов и нехватка возможностей к масштабированию VPN-серверных узлов. Там, где проектирование инфраструктуры велось в расчете на частичный дистанционный допуск (максимум 20 % пользователей синхронно), внезапный всплеск коннектов вел к критическому возрастанию задержек, обрыву сеансов связи и даже полной недоступности сервиса. К тому же образовательные институции встретились со сложностями организации юзерской поддержки: немалая часть обучающихся и педагогов ощущала трудности с инсталляцией клиентского ПО, конфигурацией протоколов и нейтрализацией локальных барьеров со стороны интернет-провайдеров (к примеру, запрет на трафик UDP). Эти выводы обусловили пересмотр стратегий: теперь в ходе внедрения VPN предписывается закладывать запас по продуктивности не ниже 50 % от максимальной прогнозируемой посещаемости[64].

Применение VPN в учебном деле дает спектр весомых плюсов. Во-первых, это рост приватности и цельности образовательного и управленческого контента: кодирование трафика обессмысливает пассивное прослушивание в местах подключения. Во-вторых, расширение горизонтов доступа к фондам для иногородних и заочников: они обретают легальный пропуск к лицензионным источникам данных и внутрисетевым порталам из произвольной географической точки. В-третьих, концентрация управления разрешениями и протоколирование входа в сеть: управленец способен в произвольный момент проконтролировать, кто, в какой период и к каким сервисам контактировал сквозь VPN, что принципиально для служебных расследований происшествий. Помимо того, VPN содействует выполнению предписаний надзорных структур (Роскомнадзора, ФСТЭК) касаемо обороны личных данных в условиях удаленной занятости.

Технология VPN превратилась в имманентную составляющую актуальной образовательной экосистемы, в особенности на этапе движения к гибридной и дистанционной моделям преподавания. При грамотном проектировании и неуклонном соблюдении правовых норм VPN синхронно повышает степень защищенности оборота личных данных и расширяет доступность учебных материалов для территориально распределенных участников. Наибольшую результативность показывает интегрированная методология, совмещающая инженерные барьеры (передовые протоколы шифрования, многофакторная аутентификация, разделение туннелирования, горячее резервирование серверных мощностей) с менеджерскими шагами (формирование локальных регламентов, тренинги для юзеров, систематический мониторинг). Обособленного анализа требует правовая плоскость: учреждения образования призваны однозначно дифференцировать дозволенные мотивы задействования VPN (оборона данных, допуск к лицензируемым источникам) и пресекать его эксплуатацию ради преодоления установленных законом барьеров. Будущие научные изыскания могут быть сориентированы на исследование влияния разных VPN-протоколов на стабильность видеоконференцсвязи и на создание динамических алгоритмов выравнивания трафика в моменты пиковой востребованности (зачетные недели, централизованные аттестации), а равно на выработку инструктивных комплексов по обучению контингента безопасной практике работы с VPN в рамках академической среды.

[63] О персональных данных : Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 21.02.2024) // СПС «Гарант» (дата обращения: 10.04.2026).

[64] Characterizing the VPN Ecosystem in the Wild // arXiv. URL: https://arxiv.org/abs/2302.06566 (дата обращения: 10.04.2026).

УДК 621.311:004.056(045)

М. З. оглы Гасанли,
обучающийся 2 курса Института права,
социального управления и безопасности ФГБОУ ВО «УдГУ».
Научный руководитель: Т. Н. Стерхова, канд. техн. наук, доцент
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Физическая безопасность источников питания: атаки через электросеть

Когда говорят о защите информационных систем, разговор почти неизбежно сводится к антивирусам, межсетевым экранам и политикам паролей. Физическая составляющая если и упоминается, то в контексте замков на серверных и видеонаблюдения. Между тем у каждого вычислительного устройства есть кое-что, на что в этом разговоре почти никогда не обращают внимания: шнур питания. А он, как выясняется, заслуживает отдельного разговора.

Дело в том, что цифровые схемы не потребляют ток равномерно. Транзистор тратит энергию именно в момент переключения из нуля в единицу или обратно. Сколько переключений произошло в данный момент и какие именно, определяется тем, какие данные обрабатываются. Это означает, что осциллограмма тока в цепи питания несёт в себе информацию о вычислениях. Явление называется утечкой через боковой канал, и от него не спасает никакая математическая стойкость шифра, потому что это не атака на алгоритм, а атака на его физическую реализацию.[65]

В 1999 году Пол Кохер вместе с коллегами опубликовал работу, которая наглядно показала, что из этого следует[66]. Они описали дифференциальный анализ мощности, DPA, и продемонстрировали: устройство с правильно реализованным AES можно вскрыть, просто понаблюдав за потреблением тока при нескольких тысячах шифрований. Для индустрии это был неприятный сюрприз.

Атаки этого класса делятся на две разновидности. Первая называется простым анализом мощности, SPA. Здесь не нужно ничего считать статистически: берёшь осциллограмму и смотришь. Работает там, где разные операции алгоритма имеют явно различимые профили потребления. Хрестоматийный пример это RSA с алгоритмом «квадрат-и-умножение»: умножение и возведение в квадрат потребляют по-разному, и биты ключа на осциллограмме видны почти буквально[67]. Вторая разновидность, DPA, куда изощрённее. Атакующий собирает большую выборку трасс при разных входных данных, выдвигает гипотезы о возможных значениях байтов ключа и ищет статистическую корреляцию между предсказанным поведением и реально измеренным потреблением[68]. Метод хорошо переносит шум: чем больше трасс, тем чище сигнал. Именно поэтому DPA остаётся применимым даже при измерении через розетку, а не напрямую на выводах микросхемы, несмотря на то что помех в электросети несравнимо больше.

Совершенно иначе устроен второй класс атак – активное воздействие на питание, известное под названиями voltage glitching или fault injection. Здесь цель не подслушать, а сломать – причём сломать предсказуемым образом[69]. Процессор при этом может пропустить инструкцию, выполнить её с ошибкой или вообще попасть в состояние, которое разработчик не закладывал. На практике этот метод применялся против смарт-карт: счётчик неверных попыток ввода PIN попросту переставал срабатывать из-за намеренно внесённого сбоя, и карта не блокировалась[70]. Компания Riscure, занимающаяся оценкой аппаратной безопасности, задокументировала подобные атаки на платёжные терминалы, автомобильные блоки управления и ряд других коммерческих устройств. Через общую электросеть, без прямого доступа к цепи конкретного устройства, это сделать сложнее, но принципиально возможно.

---

[65] Standaert F.-X. Introduction to Side-Channel Attacks // Secure Integrated Circuits and Systems / ed. I. Verbauwhede. Springer, 2010. P. 27–42.

[66] Kocher P., Jaffe J., Jun B. Differential Power Analysis // Advances in Cryptology – CRYPTO 1999. Lecture Notes in Computer Science, vol. 1666. Springer, Berlin, Heidelberg, 1999. P. 388–397.

[67] Kocher P. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems // Advances in Cryptology – CRYPTO 1996. Lecture Notes in Computer Science, vol. 1109. Springer, 1996. P. 104–113.

[68] Mangard S., Oswald E., Popp T. Power Analysis Attacks: Revealing the Secrets of Smart Cards. N.-York : Springer, 2007. 338 p.

[69] Bar-El H., Choukri H., Naccache D., Tunstall M., Whelan C. The Sorcerer's Apprentice Guide to Fault Attacks // Proceedings of the IEEE. 2006. Vol. 94, № 2. P. 370–382.

[70] Balasch J., Gierlichs B., Verbauwhede I. Electromagnetic Circuit Fingerprints for Hardware Trojan Detection // Proc. IEEE International Symposium on Electromagnetic Compatibility. 2015. P. 246–251.

Третий класс выглядит почти невероятно. Речь о передаче данных из машины, у которой нет никаких сетевых подключений вообще, ни проводных, ни беспроводных. Air gap, воздушный зазор, это традиционный способ защитить по-настоящему критичные системы. Исследовательская группа Мордехая Гури из Университета Бен-Гуриона несколько лет методично показывает, что air gap не является абсолютной защитой. Скрытые каналы находили в акустике кулеров, тепловом излучении, мерцании светодиодов[71]. Нашли и в силовой линии. Атака PowerHammer работает так: вредоносная программа на изолированной машине управляет загрузкой процессора по определённому расписанию и создаёт тем самым модулированные изменения тока в цепи питания[72]. Эти изменения расходятся по электросети и фиксируются датчиком тока в соседней розетке, на щитке этажа или даже на вводе в здание. Скорость передачи в первом случае достигала 1000 бит/с, в последнем около 10 бит/с. Негусто, но для передачи ключа вполне достаточно.

Отдельного внимания заслуживает атака PLATYPUS, опубликованная в 2021 г. исследователями из Грацского технического университета и ряда других организаций[73]. Она выбивается из общего ряда тем, что для неё не нужно ни касаться электросети, ни иметь физический доступ к машине. Оказалось, что интерфейс Intel RAPL, штатный механизм мониторинга энергопотребления процессора, был доступен непривилегированным программам и возвращал показания достаточно точно, чтобы проводить через него атаку по сторонним каналам. Фактически это классический DPA, только вместо осциллографа системный вызов. Авторам удалось восстановить ключи AES-NI и RSA. После публикации ядро Linux закрыло доступ к RAPL для обычных пользователей, Intel выпустила обновление микрокода. Схожая проблема обнаружилась и в процессорах AMD.

Защита от описанных атак не сводится к какой-то одной мере – разные классы угроз требуют разных подходов. Применительно к SPA и DPA на аппаратном уровне используются схемы с постоянным потреблением (dual-rail precharge logic): вне зависимости от обрабатываемых данных такая схема потребляет одинаковый ток в каждом такте, разрывая связь между потреблением и данными[74]. На алгоритмическом уровне применяется маскирование: перед выполнением криптографических операций данные смешиваются со случайными масками, которые затем компенсируются – в результате промежуточные значения, от которых зависит потребление, становятся случайными и не несут информации о ключе. Против voltage glitching помогают активные схемы мониторинга напряжения, отключающие устройство или сбрасывающие его состояние при выходе питания за допустимые пределы, а также LC-фильтры, подавляющие внешние помехи на входе цепи питания. Для защиты от атак типа PowerHammer рекомендуется подключать критические системы через источники бесперебойного питания с активной фильтрацией, которые физически изолируют нагрузку от внешней электросети и в таком случае изменения тока, порождаемые внутри изолированной системы, не выходят за пределы ИБП. Наконец, урок PLATYPUS состоит в том, что системные интерфейсы мониторинга энергопотребления следует рассматривать как потенциальные каналы утечки информации и ограничивать к ним доступ на уровне операционной системы.

Подводя итог, могу отметить, что атаки через канал питания представляют собой зрелую и технически разнообразную область, которая за четверть века прошла путь от лабораторной демонстрации до реальных уязвимостей в серийной продукции. Электросеть оказывается не просто инфраструктурой – она несёт в себе информацию о происходящих вычислениях и при этом может служить инструментом целенаправленного воздействия. Инцидент с PLATYPUS особенно красноречив: он показывает, что угрозы такого рода возможны даже без какого-либо физического доступа к целевой системе, а значит, модель угроз для любого устройства, выполняющего криптографические операции, должна включать канал питания в явном виде – как на этапе проектирования аппаратуры, так и при разработке системного программного обеспечения.

---

[71] Guri M., Monitz M., Mirski Y., Elovici Y. BitWhisper: Covert Signaling Channel between Air-Gapped Computers Using Thermal Manipulations // Proc. 28th IEEE Computer Security Foundations Symposium. 2015. P. 276–289.

[72] Guri M., Bykhovsky D., Elovici Y. PowerHammer: Exfiltrating Data from Air-Gapped Computers through Power Lines // IEEE Transactions on Information Forensics and Security. 2020. Vol. 15. P. 1879–1890.

[73] Lipp M., Kogler A., Oswald D., Schwarz M., Praun C., Mangard S. PLATYPUS: Software-based Power Side-Channel Attacks on x86 // Proc. 42nd IEEE Symposium on Security and Privacy (S&P 2021). P. 355–371.

[74] Chari S., Jutla C., Rao J. R., Rohatgi P. Towards Sound Approaches to Counteract Power-Analysis Attacks // Advances in Cryptology – CRYPTO 1999. Lecture Notes in Computer Science, vol. 1666. Springer, 1999. P. 398–412.

УДК 621.394.625.33:004(045)

З. Я. Давыдов, А. И. Гараев,
обучающиеся 2 курса Института права,
социального управления и безопасности ФГБОУ ВО «УдГУ».
Научный руководитель: Т. Н. Стерхова, канд. техн. наук, доцент
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Исследование дешифраторов в цифровых системах

Когда знакомишься с цифровой схемотехникой, дешифраторы поначалу кажутся чем-то простым – ну, преобразуют код в активный сигнал и всё. Но чем глубже вникаешь в их устройство, тем яснее становится, насколько они важны для построения любой сложной цифровой системы[75]. Без дешифраторов невозможно организовать ни адресацию памяти, ни управление периферийными устройствами, ни нормальную работу процессорных схем. В данной работе мы попытались разобраться не просто в том, как дешифратор описан в учебнике, но и как он ведёт себя на практике – через моделирование реальной схемы DC 3-8 в среде Micro-Cap.

Дешифратор (Decoder, DC) – это комбинационная схема, у которой n информационных входов и до 2^n выходов: на тот выход, чей номер совпадает с поданным двоичным кодом, подаётся активный уровень[76]. Если выходов ровно 2^n, схему называют полным дешифратором; если меньше – неполным. Мы работали с полной версией DC 3-8: три входа (A_0, A_1, A_2), восемь выходов (Y_0–Y_7) и вход разрешения EN. При EN = 0 все восемь выходов находятся в неактивном состоянии независимо от кода на адресных входах. При EN = 1 активизируется выход с номером $N = 4\cdot A_2 + 2\cdot A_1 + A_0$, остальные семь остаются в нуле.

Логически каждый выход реализует конъюнкцию трёх переменных в прямом или инверсном виде, в зависимости от номера выхода[77]. Например, $Y_0 = EN\cdot\bar{A}_2\cdot\bar{A}_1\cdot\bar{A}_0$, а $Y_7 = EN\cdot A_2\cdot A_1\cdot A_0$. Каждая из восьми функций является одновременно минимальной ДНФ и минимальной КНФ, т. е. упрощать их попросту некуда – они уже оптимальны. Именно поэтому дешифратор в паре с элементом ИЛИ позволяет реализовать произвольную логическую функцию от n переменных без какого-либо синтеза: достаточно подать на ИЛИ номера тех минтермов, на которых функция равна единице. Например, функция $F = A_2\cdot A_1 + \bar{A}_2\cdot A_0$ принимает значение 1 на минтермах 1, 3, 6 и 7, значит $F = Y_1 + Y_3 + Y_6 + Y_7$.

Помимо реализации отдельных функций, набор дешифраторов образует программируемую логическую матрицу (ПЛМ)[78]. В ПЛМ матрица И заменяется набором дешифраторов, формирующих все минтермы, а матрица ИЛИ программируется под нужные функции. Именно этот принцип лежит в основе современных ПЛИС (программируемых логических интегральных схем), широко применяемых в автоматизированных системах управления энергетическими объектами. Таким образом, изучение дешифратора – это фактически изучение фундаментального строительного блока всей современной цифровой техники.

Схему собирали на элементах семейства 74HC: три инвертора 74HC04 с задержкой распространения около 10 нс и восемь четырёхвходовых элементов И 74HC08 с задержкой около 15 нс[79]. Выбор именно этого семейства объясняется совместимостью с TTL-логикой, низким потреблением тока и диапазоном питания 2–6 В. Теоретическая задержка схемы составляет $t_п = 2\cdot t_{инв} + t_И = 2\cdot 10 + 15 = 35$ нс, однако из-за перекрытия фронтов реальная задержка оказывается несколько меньше.

Моделирование проводилось в Micro-Cap в режиме Transient Analysis[80]. Длительность симуляции составила 200 мкс, шаг интегрирования – 0,1 нс, напряжение питания – 5 В, нагрузочная ёмкость выходов – 15 пФ. Периоды тактовых сигналов задавались так, чтобы за 80 мкс последовательно перебирались все восемь комбинаций: A_0 – 20 мкс, A_1 – 40 мкс, A_2 – 80 мкс; EN оставался активным на протяжении всего эксперимента, кроме специального теста на блокировку.

---

[75] Угрюмов Е. П. Цифровая схемотехника : учеб. пособие. 3-е изд. СПб. : БХВ-Петербург, 2010. 800 с.
[76] Токхайм Р. Основы цифровой электроники. М. : Мир, 1988. 392 с.
[77] Хилл Дж., Питерсон Г. Введение в логическое проектирование. М. : Радио и связь, 1981. 352 с.
[78] Самофалов К. Г. Прикладная теория цифровых автоматов. Киев : Вища школа, 1987. 375 с.
[79] Шевкопляс Б. В. Микропроцессорные структуры. М. : Военное изд-во, 1990. 512 с.
[80] Новиков Ю. В. Основы цифровой схемотехники. М. : Мир, 2001. 379 с.

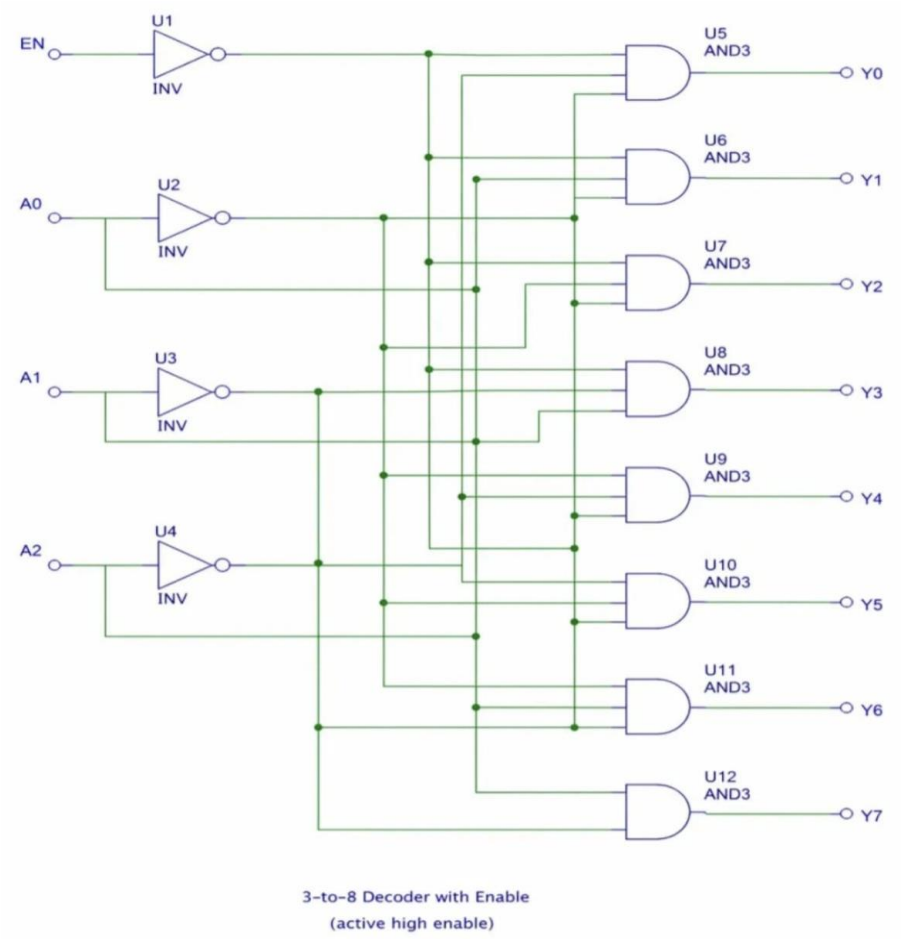


Рис. 1. Схема дешифратора DC 3-8 на логических элементах

Результаты моделирования полностью совпали с теоретической таблицей истинности: при каждой из восьми комбинаций входного кода активировался строго один выход, при EN = 0 все выходы блокировались (табл. 1).

Таблица 1

Экспериментальная таблица истинности DC 3-8

EN	A_2	A_1	A_0	Y_0	Y_1	Y_2	Y_3	Y_4	Y_5	Y_6	Y_7	N
0	X	X	X	0	0	0	0	0	0	0	0	—
1	0	0	0	1	0	0	0	0	0	0	0	0
1	0	0	1	0	1	0	0	0	0	0	0	1
1	0	1	0	0	0	1	0	0	0	0	0	2
1	0	1	1	0	0	0	1	0	0	0	0	3
1	1	0	0	0	0	0	0	1	0	0	0	4
1	1	0	1	0	0	0	0	0	1	0	0	5
1	1	1	0	0	0	0	0	0	0	1	0	6
1	1	1	1	0	0	0	0	0	0	0	1	7

Что касается временны́х задержек, то результаты вышли вполне предсказуемыми (таблица 2). Задержка по адресному входу (28 нс) оказалась чуть выше расчётной (25 нс), что объясняется реальным перекрытием фронтов при последовательном прохождении сигнала через два каскада инверторов и элемент И[81]. При этом задержка по входу EN равна расчётной: здесь сигнал проходит лишь через один элемент И, без предварительного инвертирования, поэтому паразитные эффекты менее выражены. Времена нарастания и спада (по 3 нс) хорошо соответствуют паспортным данным семейства 74HC при ёмкостной нагрузке 15 пФ.

[81] Угрюмов Е. П. Указ. соч. С. 214–218.

Таблица 2

Временны́е параметры дешифратора DC 3-8

Параметр	Значение	Примечание
tpd (EN→Y)	25 нс	задержка по входу разрешения
tpd (A→Y)	28 нс	задержка по адресному входу
tr	3 нс	время нарастания сигнала
tf	3 нс	время спада сигнала
tpd (расчёт)	25 нс	2×tинв + tИ = 2×10 + 15 нс

Отдельно стоит упомянуть возможность каскадирования. Если требуется большее число адресных входов, два дешифратора DC 3-8 легко объединяются в DC 4-16: старший разряд A_3 подаётся прямо на вход EN одной микросхемы и инверсно – на EN другой[82]. При $A_3 = 0$ активна первая микросхема (выходы Y_0–Y_7), при $A_3 = 1$ – вторая (Y_8–Y_{15}). Аналогичным образом из четырёх DC 3-8 строится DC 5-32, из восьми – DC 6-64. Такой подход широко используется в схемах адресации ОЗУ и ПЗУ: дешифраторы формируют сигналы выборки кристалла для каждого банка памяти.

Ещё одно применение дешифратора с входом разрешения – режим демультиплексора. Если вход EN использовать как информационный вход D, а адресными входами задавать номер выходного канала, схема начинает работать как коммутатор 1-на-8[83]. Через адресные входы выбирается нужный канал, и входной сигнал появляется ровно на одном выходе, тогда как остальные семь остаются в нуле. В системах телеметрии электроэнергетики это удобно для распределения одного информационного потока от датчика по нескольким линиям связи с диспетчерским пультом.

Таким образом, в ходе работы были изучены принципы построения дешифратора DC 3-8, выполнено моделирование схемы в Micro-Cap и получены экспериментальные данные, полностью соответствующие теории. Были измерены ключевые временны́е параметры схемы, показана возможность каскадирования для увеличения разрядности, а также рассмотрен режим демультиплексирования. Дешифратор оказывается гораздо более универсальным устройством, чем кажется поначалу: он выступает и как инструмент для реализации произвольных логических функций, и как базовый элемент систем адресации памяти, и как коммутатор информационных потоков. Компьютерное моделирование показало себя эффективным методом исследования, позволяющим быстро проверить корректность схемотехнических решений без сборки физического макета.

УДК [004.85+004.89]:[81'322.2](045)

Е. Ю. Егоров,
обучающийся 2 курса Института права,
социального управления и безопасности ФГБОУ ВО «УдГУ».
Научный руководитель: Т. Н. Стерхова, канд. техн. наук, доцент
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Создание языковой модели с долгосрочной памятью

В условиях большого роста объемов данных, генерируемых искусственным интеллектом, классические подходы к машинному обучению и анализу текстов сталкиваются с серьезными проблемами. Одной из наиболее сложных задач в области искусственного интеллекта является создание систем, способных не только обрабатывать информацию в моменте, но и сохранять контекст на протяжении длительного времени. Для важных отраслей, где требуется непрерывный мониторинг и анализ данных во времени (например, глубокий анализ сетевого трафика на наличие скрытых стеганографических аномалий или APT-атак), использование больших языковых моделей (LLM) ограничено их фундаментальной архитектурой.

[82] Шевкопляс Б. В. Микропроцессорные структуры. М. : Военное изд-во, 1990. С. 178.
[83] Хилл Дж., Питерсон Г. Введение в логическое проектирование. М. : Радио и связь, 1981. С. 96.

Главной проблемой современных LLM, построенных на базе классической архитектуры Transformer, является строго фиксированный размер контекстного окна. Базовый механизм внутреннего внимания (Self-Attention) вычисляет зависимости между всеми токенами в последовательности, что требует вычислительных ресурсов, возрастающих квадратично по отношению к длине входных данных. Математически это выражается формулой:

$$Attention(Q, K, V) = softmax\left(\frac{QK^T}{\sqrt{d_k}}\right)V$$ [84]

Где Q (Query), K (Key) и V (Value) представляют собой тензоры запросов, ключей и значений, а d_k – размерность вектора ключа. При попытке масштабировать контекст для анализа непрерывных потоков данных вычисление произведения QK^T приводит к экспоненциальному расходу оперативной памяти и видеопамяти (VRAM).

Популярный метод обхода этого ограничения – Retrieval-Augmented Generation (RAG) – решает задачу лишь частично. RAG фрагментирует данные и осуществляет поиск по векторному сходству, однако при таком подходе разрушается хронологическая и логическая связность событий. Модель получает разрозненные куски информации, теряя возможность отследить долгосрочные паттерны и причинно-следственные связи.

Для преодоления проблемы в рамках данного исследования рассматривается создание языковой модели с интеграцией долгосрочной памяти, базирующейся на концепциях архитектуры Titans. В отличие от механизмов статического кэширования (KV Cache), концепция долгосрочной памяти предлагает использование динамического модуля памяти (Memory as Context, MAC).

В процессе алгоритма обучения учится отфильтровывать лишнюю информацию. Он извлекает только значимые закономерности, избирательно корректируя весовые коэффициенты увеличения памяти, что надежно защищает ее от зашумления бесполезными данными.

Математический пересчет состояния памяти выглядит следующим образом:

$$M_t = LayerNorm(M_{t-1} + \sigma(W_m \cdot [M_{t-1}, x_t] + b_m))$$ [85]

Где M_t и M_{t-1} отражают новое и предыдущее состояние, x_t выступает в роликах векторного представления (эмбеддинга) текущего входа, тогда как W_m и b_m мы являемся достоверными параметрами. Подобный подход дает возможность накапливать полезную информацию, избегая проблем с затруднением буфера.

Отдельной проблемой остается запуск таких ресурсоемких систем на пользовательском железе. Если мы хотим развернуть LLM с увеличением локальной памяти (например, на видеоускорителе с 8 ГБ видеопамяти), не обойтись без специальных средств оптимизации. Одним из удачных решений в этой сфере является фреймворк Mirage. Его главная задача – грамотно оптимизировать вычислительные тензорные графики и автоматически переносить нагрузку на память GPU.

На практике подобные решения могут кардинально ускорить работу программистов, помочь в глубоком поведенческом анализе и значительно усилить информационную безопасность. Например, благодаря удерживанию широкого контекста, модель способна разделить между собой разрозненные фрагменты текста. Она может заметить даже такие неочевидные аномалии, как внедренные невидимые символы Unicode (символы нулевой ширины), с помощью которых злоумышленники часто организуют скрытые стеганографические каналы утечки данных. Обычные нейросети с их узким контекстным окном на такое просто не способны.

Подводя итог, можно сказать, что простое механическое открытие контекстного окна – не самый сильный путь. Настоящий шаг вперед заключается именно во внедрении принципов расширения памяти. Симбиоз новых вроде архитектуры Титанов и оптимизаторов уровня Mirage позволяет наконец-то создавать по-настоящему независимых ИИ-агентов. Они могут работать прямо за компьютером пользователя, не теряя ни обсуждения даже во время очень длительных рабочих сессий.

[84] Attention Is All You Need / A. Vaswani [et al.] // Advances in Neural Information Processing Systems. 2017. Vol. 30. P. 5998–6008.

[85] Titans: Learning to Memorize at Scale / S. Google Research [et al.] // arXiv preprint. 2024. URL: https://arxiv.org/html/2501.00663v1 (дата обращения: 23.05.2026).

УДК 621.375:004.056(045)

Е. Р. Ефимова,
обучающаяся 2 курса Института права,
социального управления и безопасности ФГБОУ ВО «УдГУ».
Научный руководитель: Т. Н. Стерхова, канд. техн. наук, доцент
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Операционный усилитель как цифровой детектор атак: мониторинг вольт-амперной характеристики двухполюсника в реальном времени

Микропроцессорные устройства релейной защиты и автоматики (РЗА) входят в состав критической информационной инфраструктуры[86]. Помимо кибератак через цифровые каналы, остается риск физического воздействия на дискретные цепи управления, например, отключение выключателей, приводов или сигнализации. Злоумышленник может, например, зашунтировать цепь, поставить диод последовательно или подключить конденсатор, который изменит логику работы защиты[87]. В современных терминалах РЗА не предусмотрены встроенные средства, позволяющие выявить такие вмешательства[88].

В этой работе ставится задача разработать способ быстрого обнаружения изменений вольт-амперной характеристики (ВАХ) двухполюсника с использованием операционного усилителя, чтобы детектировать атаки на цепи РЗА.

1. *Физические атаки: угрозы, цели, кража информации.* Физические атаки требуют физического доступа к оборудованию. Их используют для промышленного шпионажа, например, чтобы узнать настройки защит, а также для подготовки к кибератакам: собирают данные перед удалённым взломом, как это было при атаках на польскую энергетику в 2025 г. Иногда цель, саботаж, например, отключение энергии, или кража интеллектуальной собственности: схем, алгоритмов РЗА.

При таких действиях злоумышленник может получить логику работы защит (например, анализируя сигналы в цепях управления с помощью осциллографа), узнать режимы работы энергосистемы (отследить моменты срабатывания) и параметры настройки, измерить пороги и задержки. Всё это помогает спланировать кибератаку или обойти защиту.

Разрабатываемый детектор реагирует на вмешательство ещё на ранней стадии, пока информация не была похищена.

2. *Теоретическое обоснование метода мониторинга ВАХ.* В основе метода лежит измерение ВАХ двухполюсника, то есть зависимости тока от напряжения. Каждый тип цепи имеет уникальную ВАХ: резистор (прямая линия), диод (порог 0,6 В), конденсатор (петля гистерезиса)[89].

Эталонная ВАХ исправной цепи. Нормальной цепью РЗА принято считать активное сопротивление. Её ВАХ линейна: ток пропорционален напряжению. Эталон запоминается при калибровке.

Для измерения тока используется метод шунта, а именно последовательное включение резистора 0,01-0,1 Ом. Падение напряжения $U_{шунт} = I \times R_{шунт}$ требует усиления[90]. Операционный усилитель работает как разностный усилитель. Передаточная функция: $V_{out} = I \times R_{шунт} \times (R_4/R_3) + V_{ref}$[91]. Критическое условие точности: $R_1 = R_3$ и $R_2 = R_4 (R_2/R_1 = R_4/R_3)$.

---

[86] Технические требования к микропроцессорным устройствам релейной защиты и автоматики : СТО 56947007-29.120.70.241-2017. (с изм. 2019 г.). URL: https://docs.cntd.ru/ (дата обращения: 19.04.2026).

[87] Об утверждении дополнительных требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры, функционирующих в сфере электроэнергетики : приказ Минэнерго России от 26.12.2023 № 1215. // СПС «КонсультантПлюс» (дата обращения: 19.04.2026).

[88] Ванин В. К., Павлов Г. М. Релейная защита на элементах вычислительной техники. 2-е изд., перераб. и доп. Л. : Энергоатомиздат, 1991. С. 112–115.

[89] Титце У., Шенк К. Полупроводниковая схемотехника : справочное руководство : в 2 т. / пер. с нем. 12-е изд. М. : ДМК Пресс, 2018. Т. 1. С. 210–245.

[90] Глазырин В. Е., Литвинов И. И., Купарев М. А. Элементы автоматических устройств на микроэлектронной базе : учебник. Новосибирск : Изд-во НГТУ, 2023. С. 98–102. URL: https://www.publish.nstu.ru/catalog/uchebniki-ngtu/2801/ (дата обращения: 19.04.2026).

[91] Блоки измерительные релейных защит Ф191 : сертификат об утверждении типа средств измерений № 42141. Федеральный информационный фонд по обеспечению единства измерений. 2011. URL: https://fgisarshin.ru/bloki-izmeritelnye-relejnyh-zashhit-f191 (дата обращения: 19.04.2026). С. 3.

3. *Схема и её работа.*

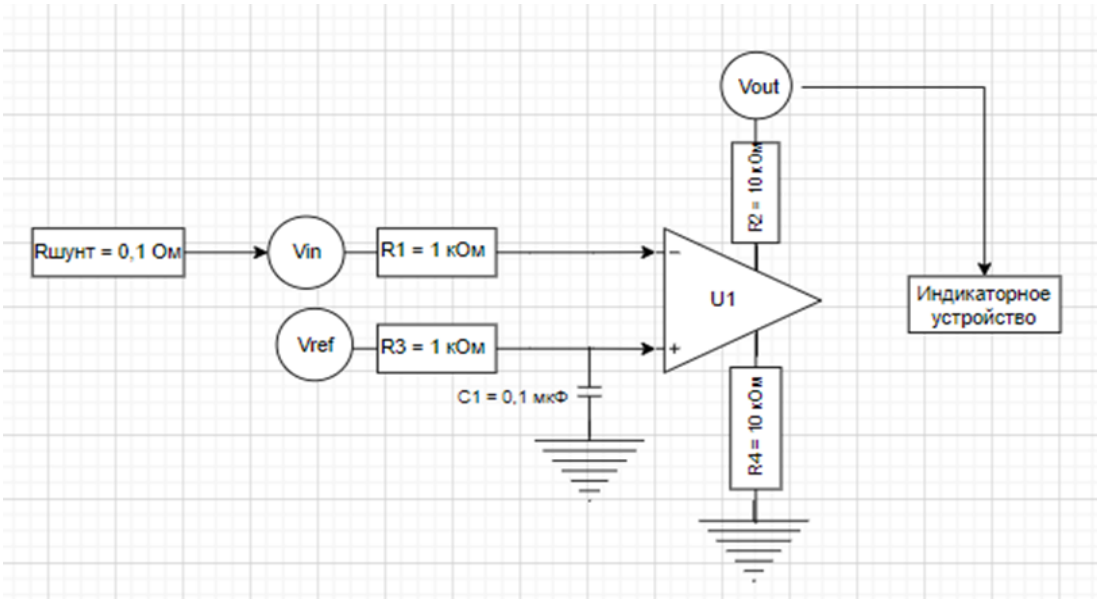


Рис. 1. Принципиальная схема детектора атак (разностный усилитель)

Схема детектора (рис. 1) разработана на основе классического разностного усилителя, описанного в учебниках Хоровица и Хилла, а также Титце и Шенка[92]. Для адаптации мониторинга цепей РЗА добавлены резистор $R_{шунт}$ и индикаторное устройство на вход и выход соответственно. Схема нарисована в draw.io, бесплатном онлайн-редакторе для создания векторных электрических схем.

Контролируемый двухполюсник подключается последовательно с шунтом R_i=0,1 Ом. Ток $I_{нагр}$ создаёт на шунте $U_{шунт} = I \times 0{,}1$. Напряжение с верхней точки шунта подаётся на неинвертирующий вход ОУ через R_1=1 кОм. Напряжение с нижней точки (земля) на инвертирующий вход через R_3=1 кОм. ОУ усиливает разность. Коэффициент усиления $R_2/R_1=R_4/R_3=10$. Выходное напряжение V_{out} пропорционально току. При изменении ВАХ в результате атаки V_{out} меняется.

Выполнена в draw.io. Обозначения: U_1 (LM358); R_1,R_3=1 кОм; R_2,R_4=10 кОм; $R_{шунт}$=0,1 Ом; C_1=0,1 мкФ; V_{in} (вход с шунта); V_{out} (выход на индикаторное устройство).

4. *Моделирование атак.* На вход подавался синус 1 В, 50 Гц. Нагрузка $R_{нагр}$=100 Ом имитировала исправную цепь РЗА.

Нормальный режим. Ток протекает через $R_{нагр}$ и $R_{шунт}$. V_{out} повторяет форму входного сигнала. При нормальной работе ВАХ представляет собой прямую линию, выходящую из нуля. Это соответствует линейной зависимости тока от напряжения в резистивной цепи.

Атака «Параллельный шунт». Дополнительный резистор $R_{атаки}$=10 Ом подключается параллельно $R_{нагр}$: один вывод к точке между источником и $R_{нагр}$, второй с землёй. Общее сопротивление падает: $R_{общ} = (100\times10)/(110) \approx 9{,}09$ Ом. Ток возрастает в 11 раз. Наклон ВАХ увеличивается. V_{out} резко падает.

Атака «Последовательный диод». Диод 1N4148 включается последовательно в разрыв цепи между $R_{нагр}$ и $R_{шунт}$. Анод подключен к $R_{нагр}$, катод к $R_{шунт}$. До 0,6 В диод закрыт, ток = 0. После превышения порога диод открывается. На ВАХ появляется «ступенька»: при напряжении ниже 0,6 В ток = 0, затем следует резкий скачок. V_{out} = 0 до порога, затем скачок.

Атака «Подключение конденсатора». Конденсатор $C_{атаки}$=100 мкФ подключается параллельно $R_{нагр}$ (один вывод к точке между источником и $R_{нагр}$, второй – к земле). При подаче напряжения конденсатор заряжается (ток сначала большой, потом падает), при снятии – разряжается. ВАХ приобретает вид петли гистерезиса, ветви заряда и разряда не совпадают. V_{out} имеет экспоненциальную форму.

5. *Риски физических атак и алгоритм детектирования.* Риски: нарушение функционирования (шунт блокирует команду отключения, авария не отключается); искажение информации (диод или конденсатор меняют логику защиты, защита срабатывает неверно); утечка конфиденциальной информации (подключение измерительного оборудования раскрывает логику и параметры защит); подготовка к кибератаке (сбор информации об уязвимостях создаёт предпосылки для комбинированной атаки).

[92] Хоровиц П., Хилл У. Искусство схемотехники : в 2 т. Пер. с англ. 6-е изд., перераб. М. : Мир, 2015. Т. 1. С. 245–260.

Алгоритм детектирования: калибровка (при исправной цепи запоминается эталонное V_{out}); мониторинг (непрерывное измерение V_{out}); сравнение (если отклонение >5 % от эталона – аномалия); тревога (сигнал на светодиод, реле или SCADA).

6. *Достоинства, ограничения и заключение.* Достоинства: низкая стоимость (менее 100 руб.), простота изготовления, обнаружение трёх типов атак, широкий диапазон температур (от –40°C до +125°C).

Ограничения: точность зависит от качества резисторов, ограниченный диапазон токов, необходимость гальванической развязки для защиты от высокого напряжения в цепях РЗА.

Разработан метод мониторинга ВАХ двухполюсника на операционном усилителе. Схема выполнена в draw.io на основе классических решений, описанных в учебниках Хоровица и Хилла, а также Титце и Шенка. Рассмотрено моделирование трёх атак, определены диагностические признаки каждой. Устройство может применяться для непрерывного контроля цепей РЗА, обнаружения вмешательства (саботаж или кража информации) и интеграции в существующие терминалы. Перспективы: повышение точности, интеграция с микроконтроллерами, протокол оповещения в SCADA.

УДК 621.311:004.056(045)

М. А. Зараев,
обучающийся 2 курса Института права,
социального управления и безопасности ФГБОУ ВО «УдГУ».
Научный руководитель: Т. Н. Стерхова, канд. техн. наук, доцент
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Обеспечение целостности циклов синхронизации времени как критический фактор предотвращения аварий в электроэнергетике

Современные цифровые подстанции в электроэнергетике предъявляют принципиально новые требования к точности синхронизации времени. Если в повседневной жизни ошибка в несколько секунд не имеет серьёзных последствий, то в системах релейной защиты и противоаварийной автоматики погрешность в микросекунды может привести к ложному отключению линии или несрабатыванию защиты при реальной аварии. Целью настоящей статьи является обоснование того, что обеспечение целостности циклов синхронизации времени является критическим фактором предотвращения аварий в электроэнергетике, поскольку потеря микросекундной точности равноценна физическому повреждению первичного оборудования.

Физическая основа проблемы связана с тем, как измеряется электрический ток на цифровых подстанциях. Внутри подстанции устанавливаются так называемые мерцающие блоки (Merging Units), которые берут аналоговый сигнал тока с высоковольтных трансформаторов и превращают его в цифровые отсчёты («семплы»). Чтобы релейная защита на другом конце линии правильно сравнила токи, эти отсчёты должны быть сделаны строго одновременно.

Учёный по имени Й. Ли и его коллеги выяснили, что в энергетике очень важно, чтобы все устройства на подстанциях показывали идеально точное время. И лучший способ этого добиться – использовать специальный протокол PTP, его проверили специальным методом «аппаратура в контуре»[93].

Обычные компьютерные протоколы, например NTP (тот, что синхронизирует время в интернете), работают с точностью до тысячных долей секунды (миллисекунд). Для простых задач – например, чтобы понять, в какой последовательности произошли события – этого хватает. Но для систем релейной защиты (которые отключают аварии за доли секунды) такая точность никуда не годится – она слишком грубая.

Поэтому для энергетики придумали специальный протокол PTP (Precision Time Protocol). Он даёт точность уже до миллионных долей секунды (микросекунд). Для него есть специальный стандарт IEEE C37.238-2017, который прописывает, как именно применять PTP на цифровых подстанциях[94]. Это делает правила синхронизации едиными для всех.

[93] Ли Й. Повышение точности синхронизации времени в электроэнергетических системах: решение на основе PTP с тестированием по схеме «аппаратура в контуре» / Й. Ли, А. Эстебсари, Р. Хоптрофф [и др.] // IEEE Transactions on Industry Applications. 2025. Т. 62, № 2. С. 2062–2065. URL: https://researchportal.lsbu.ac.uk/ (дата обращения: 20.04.2026).

[94] IEEE C37.238-2017. IEEE Standard Profile for Use of IEEE 1588 Precision Time Protocol in Power System Applications. IEEE, 2017. С. 5–12. URL: https://standards.ieee.org/ieee/C37.238/6650/ (дата обращения: 20.04.2026).

А самый главный мировой стандарт для цифровых подстанций – это серия IEC/IEEE 61850. Внутри неё есть документ IEC/IEEE 61850-9-3:2016, который уточняет, как именно использовать PTP на так называемой шине процесса[95].

Для владельцев цифровых подстанций важно понимать роли устройств в PTP. Главные часы (Grandmaster) обычно получают сигнал от спутников GPS или ГЛОНАСС. Промежуточные часы (Boundary Clock) переиздают синхронизацию внутри подстанции. Коммутаторы с функцией Transparent Clock сообщают, насколько они сами задержали пакет. Как указано в IEC TR 61850-90-4:2020, при проектировании сетей цифровых подстанций необходимо учитывать архитектуру синхронизации и задержки, вносимые сетевым оборудованием[96].

Технический комитет IEC также разработал специальный документ IEC TS 60255-216-1:2025, который устанавливает общие требования и испытания функций защиты с использованием цифровой связи на входе и выходе, включая требования к синхронизации[97]. Кроме того, в IEC TS 63266:2023 представлены современные подходы к представлению связи при автоматизации электроэнергетики, что также влияет на способы передачи меток времени[98].

К числу практических преимуществ точной синхронизации относятся: корректная работа дифференциальной защиты линий без ложных отключений; высокая точность определения места повреждения (погрешность в 1 мкс даёт ошибку всего в 300 метрах для воздушной линии); возможность восстановления точной последовательности срабатываний устройств при аварии.

Вместе с тем существуют и недостатки, о которых необходимо знать. Во-первых, зависимость от спутников: потеря GPS/ГЛОНАСС из-за глушения или помех переводит систему в режим удержания, и со временем ошибка нарастает. Во-вторых, возможны скачки времени при переключении на резервный Grandmaster, что может дестабилизировать защиту. В-третьих, высокая стоимость высокоточных генераторов.

С физической точки зрения потеря синхронизации не проходит бесследно. Каждый микросекундный сдвиг между семплами токов на разных концах линии превращается в кажущуюся разницу токов. Сдвиг в 10 микросекунд для сети 50 Гц соответствует фазовому сдвигу около 0,18 градуса. Этого достаточно, чтобы дифференциальная защита с высокочувствительной уставкой приняла решение на отключение. Сдвиг в 100 мкс – это уже гарантированное ложное срабатывание и отключение здорового оборудования.

Перспективным направлением является использование квантовых технологий для синхронизации. Как показано в работе Ю. Чэнь и соавторов, квантово-коммуникационная платформа синхронизации может быть применена для распределённых трёхмерных моделей энергосетей в мультирегиональных диспетчерских центрах, что открывает новые возможности для обеспечения целостности циклов синхронизации[99].

Российскими исследователями также активно изучаются вопросы синхронизации в электроэнергетике. Н. Г. Губанов и А. С. Рагузин провели анализ и моделирование протоколов синхронизации в информационной системе региональной электросетевой компании и подтвердили, что для задач релейной защиты и противоаварийной автоматики[100] обязательно нужен именно PTP.

Сегодня большинство современных цифровых подстанций уже оснащаются PTP-мастерами и поддерживающими их коммутаторами. А вот если подстанция старая и не поддерживает PTP штатно, для неё можно использовать специальные GPS-приёмники с выходом PTP либо высокоточные NTP-серверы с компенсацией задержек. Сама по себе синхронизация по PTP безопасна для устройств релейной защиты и автоматики, но только если всё правильно спроектировано. Главная опасность – скачок

---

[95] IEC/IEEE 61850-9-3:2016 – Communication networks and systems for power utility automation. Часть 9-3: Precision time protocol profile for power utility automation. IEC/IEEE, 2016. С. 8-15. URL: https://standards.ieee.org/ieee/61850-9-3/6167/ (дата обращения: 20.04.2026).

[96] IEC TR 61850-90-4:2020. Communication networks and systems for power utility automation. Часть 90-4: Network engineering guidelines. IEC, 2020. С. 34–42. URL: https://webstore.iec.ch/en/publication/64801 (дата обращения: 20.04.2026).

[97] IEC TS 60255-216-1:2025. Measuring relays and protection equipment. Часть 216-1: Digital interface – General requirements and tests for protection functions using digital communication as input and output. IEC, 2025. С. 20–25. URL: https://webstore.iec.ch/en/publication/77735 (дата обращения: 20.04.2026).

[98] IEC TS 63266:2023. Representation of communication in power utility automation. IEC, 2023. С. 15–18. URL: https://webstore.iec.ch/en/publication/68270 (дата обращения: 20.04.2026).

[99] Чэнь Ю. Quantum Communication-Assisted Synchronization Framework for Distributed 3D Power Grid Models Across Multi-Regional Control Centers / Ю. Чэнь, Цз. Люй, Р. Ху [и др.] // EAI Endorsed Transactions on Scalable Information Systems. 2026. Т. 13, № 4. С. 3–7. URL: https://publications.eai.eu/index.php/sis/article/view/12031 (дата обращения: 20.04.2026).

[100] Губанов Н. Г., Рагузин А. С. Анализ и моделирование протоколов синхронизации в информационной системе региональной электросетевой компании // Вестник Самарского государственного технического университета. Сер. «Технические науки». 2016. № 1 (49). С. 10–13. URL: https://elibrary.ru/item.asp?id=27122594 (дата обращения: 20.04.2026).

фазы в момент переключения с основного Grandmaster на резервный, поэтому для защиты от этого применяют либо алгоритмы плавного перехода, либо два независимых источника синхронизации.

На рынке есть как оригинальные решения от ведущих вендоров (полностью совместимые с конкретными терминалами защиты), так и универсальные PTP-грандмастеры. Рекомендуется выбирать сертифицированные решения стандартов IEC 61850 и IEEE 1588-2008 от проверенных производителей, обращая внимание на совместимость с терминалами защиты, тип осциллятора и наличие резервирования.

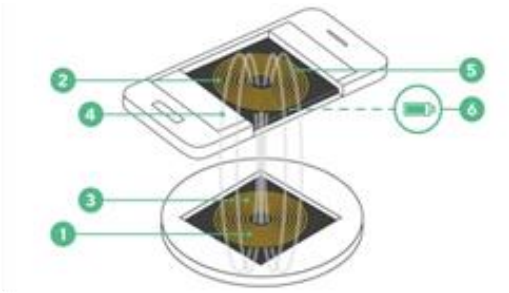
УДК 621.396.6(045)

К. Н. Зотов,
обучающийся 2 курса Института права,
социального управления и безопасности ФГБОУ ВО «УдГУ».
Научный руководитель: Т. Н. Стерхова, канд. техн. наук, доцент
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Анализ беспроводных зарядок для гаджетов

В наши дни беспроводные зарядные станции стали востребованным атрибутом для обладателей современных смартфонов, умных часов и прочих устройств. Они избавляют от постоянного подсоединения проводов и множества блоков питания с разными разъёмами. Каков принцип действия беспроводной зарядки и на какие параметры ориентироваться при покупке? Данный материал поможет разобраться во всех нюансах использования беспроводных зарядных устройств.

Принцип работы беспроводной зарядки для мобильных гаджетов базируется на двух основных элементах. Первый элемент – зарядная платформа, внутри которой находится активная индукционная катушка. При подключении питания этот компонент формирует слабое магнитное поле, действующее в радиусе примерно от 5 и максимум до 10 см. Второй важный элемент – приёмное устройство, встроенное в смартфон. Оно выполнено в виде пассивной индукционной катушки – рамки с медной обмоткой (см. рис. 1).



1. Катушка передатчика
2. Катушка приёмника
3. Ток в катушке передатчика
4. Электромагнитное поле
5. Ток в катушке приёмник
6. Зарядка аккумулятора

Рис. 1. Принципиальная схема работы беспроводной зарядки

Попадая под воздействие магнитного поля, она генерирует электрический ток, который поступает на аккумулятор[101].

Современные смартфоны в большинстве своём уже имеют встроенный «приёмник» для беспроводной зарядки (см. рис. 2).

Рис. 2. Пример «наклейки – приёмник» для беспроводной зарядки[102]

[101] Как работает беспроводная зарядка и надо ли ей пользоваться. URL: https://fumiko.ru/blog/gaydy/kak-rabotaet-besprovodnaya-zaryadka-i-nado-li-ey-polzovatsya/ (дата обращения: 22.04.2026).

Однако телефон может не поддерживать такую функцию, можно приобрести особую «наклейку», которая размещается под чехлом и соединяется с разъёмом аппарата (см. рис. 3)[103].

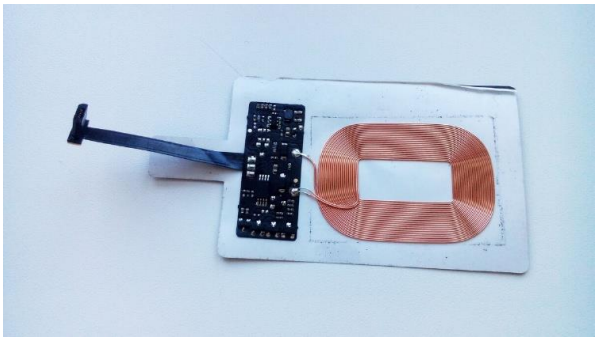


Рис. 3. Составляющие компоненты «наклейки – приёмник» для беспроводной зарядки[104]

Qi является самым распространённым стандартом. Его поддерживают практически все ведущие бренды смартфонов (см. рис. 4).

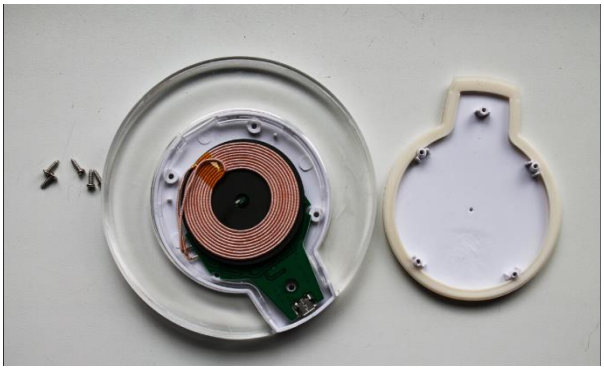


Рис. 4. Составляющие компоненты беспроводной зарядки по стандарту Qi[105]

Устройства, работающие по этому стандарту, обычно обеспечивают мощность от 5 до 15 ватт. Смартфоны в основном поддерживают 5 ватт или 7,5 ватт, однако встречаются современные модели, способные принимать от 10 до 15 ватт и выше. Зарядная станция активирует поле только после обнаружения совместимого с Qi устройства (см. рис. 5). Благодаря этому стандарт предотвращает включение зарядки при попадании в зону действия поля посторонних металлических предметов, которые иначе могли бы сильно нагреться, – так обеспечивается безопасное использование зарядного устройства. В 2023 году был представлен усовершенствованный стандарт Qi2.

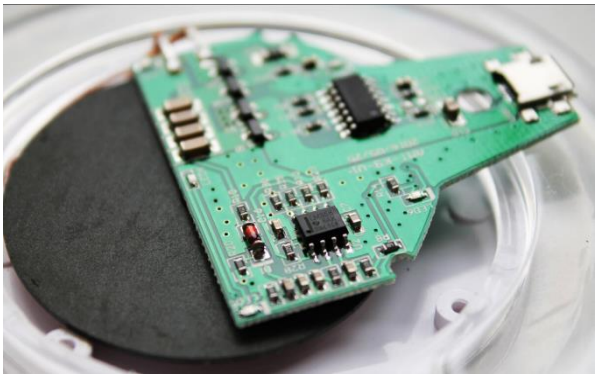


Рис. 5. Схема импульсного генератора с логикой включения отключения[106]

---

[102] Изображение «наклейки – приёмника» для беспроводной зарядки. URL: https://avatars.dzeninfra.ru/get-zen_doc/1062011/pub_5ccd93a802612c00b36f06c0_5ccd95be6f616900b21283d6/scale_1200 (дата обращения: 22.04.2026).

[103] Наклейка-приемник для беспроводной зарядки. URL: https://dzen.ru/a/XM2TqAJhLACzbwbA (дата обращения: 22.04.2026).

[104] Изображение составляющих компонентов «наклейки – приёмника» для беспроводной зарядки. URL: https://avatars.dzeninfra.ru/getzen_doc/1587012/pub_5ccd93a802612c00b36f06c0_5ccd991e7e88ed00b4f11762/scale_1200 (дата обращения: 22.04.2026).

[105] Изображение составляющих компонентов беспроводной зарядки. URL: https://avatars.dzeninfra.ru/get-zen_doc/225901/pub_5ccd93a802612c00b36f06c0_5ccd9994ffaa2300b352e31a/scale_1200 (дата обращения: 22.04.2026).

Стандарт PMA почти не имеет отличий от Qi. Разница состоит в частоте тока в катушке: если Qi работает на частоте от 100 до 205 kГц, то PMA – на от 277 до 357 kГц. Однако гаджетов, совместимых с этим стандартом, выпущено заметно меньше.

Rezence – многообещающий, но пока редко встречающийся вариант. Он мог бы быть более удобным благодаря увеличенной дистанции зарядки. В Rezence применяется эффект магнитного резонанса, поэтому энергия способна передаваться на расстояние даже сквозь небольшие преграды. С помощью станций, поддерживающих данный стандарт, можно MagSafe – разработка компании Apple, ориентированная на потребности iPhone, умных часов и наушников. Отличительная черта зарядной шайбы – наличие кольцевого магнита, окружающего обычную катушку. Задача этого стандарта – облегчить совмещение катушек для достижения более высокой скорости зарядки. В итоге мощность зарядки MagSafe достигает 15 ватт. Реальная мощность, поступающая на iPhone, зависит от блока питания и текущего состояния системы.

Достоинства и недостатки[107].

К плюсам можно отнести:

Минимальное количество проводов – отпадает необходимость каждый раз искать путающийся и вечно теряющийся кабель, когда требуется зарядить мобильное устройство.

Простота и удобство эксплуатации – достаточно лишь положить смартфон на беспроводную зарядную панель. Не требуется искать разъём и вставлять в него штекер и не всегда с первого раза это удаётся, особенно в случае с microUSB.

Если случайно дёрнуть заряжающийся телефон, зарядная станция не сломается. При неосторожном обращении с проводной зарядкой легко повредить разъём – как на кабеле, так и на самом устройстве.

Универсальность – приобретя многофункциональную беспроводную станцию, можно одновременно питать смартфон, планшет, часы, наушники и прочие гаджеты с поддержкой соответствующей технологии.

Долговечность – при бережном обращении док-станция прослужит значительно дольше, чем обычный USB-кабель.

Однако имеются и минусы:

Невысокий коэффициент полезного действия около трёх четвертых в лучшем случае. Остальная энергия рассеивается «в воздух».

Невысокая скорость зарядки – беспроводная технология заметно уступает проводной. Этот недостаток особенно ощутим для смартфонов с ёмким аккумулятором.

Не очень удобно пользоваться смартфоном в процессе зарядки: при обычной проводной зарядке можно одновременно питать устройство и работать с ним, тогда как при беспроводной приходится дожидаться окончания зарядки или мириться с неудобствами.

Дополнительные траты – необходимо покупать док-станцию отдельно, поскольку она обычно не входит в комплект телефона в отличие от USB-кабеля. К тому же качественное и надёжное устройство от известного производителя стоит довольно дорого.

Если чехол слишком толстый, он может мешать нормальной зарядке, поэтому перед установкой смартфона на док-станцию его придётся постоянно снимать.

КПД беспроводного зарядного устройства не так высок, можно сделать его более продуктивным. Дело в том, что потерянные проценты КПД не исчезают бесследно: они превращаются в основном в тепло, разогревая смартфон и зарядную станцию. Чем мощнее зарядка, тем сильнее этот эффект. Например, при 50 % потерь для 10 ваттного устройства 5 ватт уходит в тепло – этого достаточно, чтобы нагреть смартфон на от 5 до 7 градусов и негативно сказаться на сроке службы его аккумулятора. И чем выше мощность зарядного устройства, тем больше потери и сильнее нагрев[108].

Для повышения КПД производители применяют разные методы. Например, количество изменяют и размер катушек либо используют автоматическое позиционирование гаджета с помощью стационарных магнитов. Некоторые компании оснащают смартфон и зарядную станцию подвижными катушками, которые сами находят оптимальное взаимное расположение.

Безопасно ли это для вашего смартфона?

---

[106] Изображение схемы импульсного генератора с логикой включения отключения. URL: https://avatars.dzeninfra.ru/getzen_doc/1587012/pub_5ccd93a802612c00b36f06c0_5ccd99ae6f616900b21283f3/scale_1200 (дата обращения: 22.04.2026).

[107] Как работает беспроводная зарядка: технология, преимущества, безопасность // Блог М.Видео. URL: https://www.mvideo.ru/blog/pomogaem-razobratsya/kak-rabotaet-besprovodnaya-zaryadka-tehnologiya-preimushhestva-bezopasnost (дата обращения: 22.04.2026).

[108] Беспроводная передача электричества. URL: https://ru.wikipedia.org/wiki/Беспроводная_передача_электричества?ysclid=mpb0mejemr59646371XM2TqAJhLACzbwbA (дата обращения: 22.04.2026).

Беспроводная зарядка безопасна для электронных устройств, однако есть нюансы, способные навредить при неосторожном обращении. В частности, беспроводные ЗУ нагреваются – возникает нагрев из-за взаимодействия передающей и принимающей катушек.

Причём он тем сильнее, чем ниже КПД самой зарядки, но также зависит от условий эксплуатации. Из-за перегрева литий-ионные и литий-полимерные аккумуляторы быстрее изнашиваются. В результате их ёмкость заметно падает – устройство начинает хуже держать заряд. Чтобы этого избежать, можно периодически менять использование док-станции и обычного USB-кабеля.

Оригинальные беспроводные зарядные устройства полностью совместимы со смартфонами конкретного производителя, компании гарантируют их безопасность и надёжность. К тому же они стилистически сочетаются с устройствами бренда. Единственный и главный недостаток – высокая стоимость. Поэтому на рынке представлены универсальные зарядные станции. При таких же технических характеристиках они стоят значительно дешевле оригинальных. Их можно подобрать на любой вкус. При покупке неоригинального зарядного устройства рекомендуется отдавать предпочтение известным брендам: Hama, Qumo, Belkin, Xiaomi, Canyon, Rombica. Borofone, и другим.

УДК 343.13:62:004(045)

З. М. Исмагилова,
обучающаяся 4 курса Института права,
социального управления и безопасности ФГБОУ ВО «УдГУ».
Научный руководитель: Ф. А. Абашева, канд. юрид. наук, доцент
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Законодательные и теоретические основы применения современных технических средств и цифровых технологий при производстве следственных действий

Стремительное развитие цифровых технологий выступает одним из ключевых факторов, определяющих трансформацию всех сфер общественной жизни, включая уголовное судопроизводство. Современная преступность активно использует высокотехнологичные способы совершения и сокрытия противоправных деяний, что требует адекватного ответа со стороны правоохранительных органов, в том числе посредством внедрения новейших технических средств и цифровых инструментов непосредственно в процесс расследования. Как отмечает О. В. Овчинникова, цифровизацию следственных действий следует понимать как средство расширения их доказательственного потенциала, при этом закономерности применения цифровых технологий напрямую зависят от способа получения доказательственной информации[109]. Таким образом, формирование целостной законодательной базы и прочного теоретического фундамента для применения современных технологий при производстве следственных действий становится приоритетной задачей, отвечающей вызовам современности.

Теоретический базис применения технических средств и цифровых технологий в уголовном процессе базируется на фундаментальных положениях общей теории криминалистики и уголовно-процессуальной науки. В современных исследованиях выделяется несколько ключевых направлений теоретического осмысления данной проблематики.

В научной литературе разрабатывается концепция «цифровой криминалистики» как самостоятельного раздела криминалистической техники. Методологически обоснованы концептуальные положения криминалистического исследования цифровой информации, ее производных, средств обработки и защиты; с позиций криминалистической техники и тактики раскрыты особенности обнаружения, фиксации, предварительного исследования и последующего использования цифровых следов. Цифровая трансформация криминалистики, по мнению ряда авторов, должна выражаться не только в уточнении и модернизации действующих научных положений, но и в разработке принципиально новых подходов, адекватных современному уровню технологий.

[109] Овчинникова О. В. Цифровизация следственных действий: проблемы и перспективы // Вестник Челябинского государственного университета. Серия «Право». 2024. Т. 9, вып. 1. С. 51–57.

Значительный вклад в развитие теоретических основ вносят исследования, посвященные систематизации современных информационных источников, используемых следователем. Так, Д. В. Воронков и А. М. Сосновикова выделяют четыре группы технологий, применимых для повышения эффективности следственной деятельности: комплексы, направленные на автоматизацию; системы поддержки принятия решений; средства работы с компьютерной информацией; иные технологии, повышающие эффективность традиционных процессов. На основе анализа конкретных примеров авторами сформулированы ключевые принципы внедрения новых технологий: презумпция свободы следователя/дознавателя; автономность решений; сохранение значения информации при соблюдении ее целостности[110].

Отдельного внимания заслуживает теоретическая проблема определения правовой природы цифровой (электронной) информации в уголовном судопроизводстве. Как отмечает М. К. Нуркаев, имеющиеся различия в определении природы цифровой информации со стороны ученых наложили определенный отпечаток не только на представления о доказательствах и средствах доказывания среди практических работников, но и на состояние уголовно-процессуального законодательства в целом[111]. Отсутствие легальной дефиниции «электронное доказательство» существенно осложняет их понимание и использование, в связи с чем обоснованно предлагается дополнить УПК РФ соответствующей нормой.

Законодательную основу применения технических средств и цифровых технологий в следственной деятельности составляет, прежде всего, Уголовно-процессуальный кодекс Российской Федерации, который содержит ряд принципиальных положений, регламентирующих данную сферу.

Фундаментальную основу составляет ч. 6 ст. 164 УПК РФ, где в перечне общих регламентов проведения следственных мероприятий эксплицитно закреплено право на использование технических инструментов и методов для поиска, фиксации и изъятия следов преступной деятельности и вещественных доказательств. В то же время закон выдвигает императивное условие: до фактического старта следственного действия должностное лицо обязано проинформировать всех участников процесса о планируемом использовании технических средств.

Положение ст. 164.1 УПК РФ регламентирует особенности изъятия электронных носителей информации и копирования содержащейся на них информации. Так, при их изъятии должны применяться технические средства для копирования информации по ходатайству их законного владельца, а следователь вправе применить их для копирования информации, содержащейся на электронных носителях[112]. Они выделены в особый вид вещественных доказательств (п. 5 ч. 2 ст. 82 УПК РФ), что подчеркивает их специфический правовой режим.

Шаг вперёд был сделан с введением ст. 189.1 УПК РФ, разрешающей проведение с использованием систем видеоконференцсвязи трех следственных действий: допроса, очной ставки и предъявления для опознания. Это было сделано для обеспечения дистанционного участия лиц в необходимых мероприятиях, сокращения времени для проведения такого следственного действия, а также снижения нагрузки на органы предварительного следствия, при этом сохраняя гарантии прав участников.

Кроме того, в соответствии с ч. 3 ст. 170 УПК РФ закреплено требование об обязательном использовании технических средств для дополнительной фиксации результатов осмотра в случае проведения его без понятых, когда их участие затруднено или невозможно. Часть 1 ст. 58 УПК РФ определяет статус специалиста, который может привлекаться к участию в следственных действиях, в том числе для применения технических средств при исследовании материалов уголовного дела.

Развиваются и подзаконные нормативные акты. В соответствии с рядом указов Президента РФ, постановлений правительства и актов различных федеральных органов в стране происходит переход к информационному обществу, в том числе за счёт массового использования технологий искусственного интеллекта (далее – ИИ). Введена система цифровых прав и цифровых финансовых активов, что требует создания эффективной уголовно-правовой защиты современных общественных отношений от киберпреступлений.

Нормативное регулирование развивается, однако в правоприменительной практике выявляется ряд серьезных проблем, требующих научного изучения и законодательного урегулирования.

---

[110] Воронков Д. В., Сосновикова А. М. Модели использования следователем современных информационных источников ориентирующего и доказательственного значения // Правоприменение. 2026. Т. 10, № 1. С. 45–58.

[111] Нуркаева М. К. Некоторые проблемы и перспективы формирования новых следственных действий, направленных на получение цифровой информации // Правовое государство: теория и практика. 2025. № 1. С. 112–120.

[112] Уголовно-процессуальный кодекс Российской Федерации : Федеральный закон от 18.12.2001 № 174-ФЗ (ред. от 31.07.2025) // СПС «КонсультантПлюс» (дата обращения: 15.04.2026).

Одной из ключевых проблем выступает отсутствие в законодательстве легального определения понятий «цифровое доказательство» и «электронное доказательство». Как отмечается в научной литературе, отсутствие дефиниций, а также правил собирания, проверки и оценки цифровых данных создает существенные сложности в правоприменении. Э. Л. Сидоренко, в частности, указывает на непрописанность требований к допустимости цифровых доказательств и методологии их изъятия.

В результате возникает противоречие между техническим совершенствованием и устоявшимися нормами УПК РФ, регулирующими допустимость и достоверность доказательств. Основные проблемы, которые выделяют учёные и практики – это несоответствие процедур изъятия, сложности обеспечения целостности цифровой информации и оценка судом сложных алгоритмических методик.

Д. А. Сиротинин, анализируя практику дистанционного допроса, выделял ряд сложностей в реализации организационных, технических и правовых критериев в пределах, сформулированных в статье 189.1 УПК РФ. В частности, требуют разрешения вопросы фиксации хода и результатов следственного действия, а также порядка оформления и подписания протокола допроса, проводимого с использованием систем видеоконференцсвязи[113].

Следующая проблема – недостаточная урегулированность применения конкретных технических средств. Например, С. И. Грицаев с соавторами обращают внимание на необходимость интеграции специализированных интернет-ресурсов с современными базами данных и в систематизации методов их применения в следственной деятельности.

Научные исследования и реализация инженерных разработок дают несколько перспективных направлений дальнейшего внедрения цифровых технологий в следственную деятельность. Например, технологии дистанционного производства следственных действий.

Помимо уже урегулированных законодательством допроса, очной ставки и предъявления для опознания, в научной литературе описываются и иные методы производства вербальных следственных действий: компьютерно-опосредованная реальность, голография, а также разрабатываются основные положения концепции электронных следственных действий.

В процессе осмотра места происшествия используются технологии GPS и ГЛОНАСС, которые определяют с высокой точностью определять координаты приёмника и обеспечивают надёжную привязку на открытой местности. Беспилотники помогают проводить ориентирующую и обзорную фотосъёмку высокого качества. 3D-сканирование даёт возможность фиксировать место происшествия без искажений, создавать трёхмерные модели объектов и следов, а на их основе – воссоздавать детали произошедшего с помощью виртуальной реальности.

Как уже упоминалось, ИИ внедряется в деятельность правоохранительных органов. Практика показывает, что он способен сопоставлять данные из разных уголовных дел, выявлять связи между эпизодами, анализировать поведение подозреваемых и прогнозировать сценарии преступлений. Председатель Следственного комитета России А. И. Бастрыкин подтвердил, что ведомство активно применяет технологии искусственного интеллекта для выявления закономерностей преступного поведения на основе анализа материалов уголовных дел, при этом, по его словам, хоть ИИ и не сможет полностью заменить следователей, но зато позволит значительно ускорить отдельные этапы работы.

Ещё одним элементом развития является формирование Единой цифровой платформы уголовного судопроизводства, которая подразумевает модернизацию процессов через повсеместную аудиовизуальную фиксацию и четкое установление правил работы с электронными доказательствами. Внедрение этой концепции потребует смены ведомственного «туннельно-вертикального» подхода на программно-целевую модель управления ресурсами в рамках цифровизации как непосредственной следственной работы, так и всей структуры уголовной юстиции в целом.

Реализация этих направлений – от разработки программных средств до совершенствования методик – требует системного восполнения законодательных и теоретических пробелов. Сама сфера применения цифровых технологий в следственных действиях сегодня представляет собой динамичную междисциплинарную область на стыке уголовно-процессуального права, криминалистики и информационных технологий.

Действующее законодательство, прежде всего УПК РФ, содержит базовые нормы, регламентирующие возможность и порядок применения технических средств, однако стремительное технологическое развитие опережает темпы законодательных изменений. Пробелы в правовом регулировании, включая отсутствие легальных дефиниций ключевых понятий, недостаточную регламентацию процедур получения и оценки цифровых доказательств, требуют системного восполнения.

---

[113] Сиротинин Д. А. Сложности и перспективы дистанционного допроса в досудебном уголовном производстве // Бизнес. Образование. Право. 2023. № 4 (65). С. 229–233.

Теоретическая база, представленная концепциями цифровой криминалистики, системами классификации современных технологий, принципами их внедрения в следственную практику, создает научный фундамент для дальнейшего совершенствования как законодательства, так и правоприменительной деятельности. Дальнейшее развитие должно быть ориентировано на гармонизацию нормативного регулирования, углубление теоретических исследований и активное внедрение апробированных технологических решений в практику расследования преступлений.

УДК 621.373:004.056(045)

Р. С. Исупов, А. Р. Кагарманов,
обучающиеся 3 курса Института права,
социального управления и безопасности ФГБОУ ВО «УдГУ».
Научный руководитель: Т. Н. Стерхова, канд. техн. наук, доцент
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Разработка и моделирование LC-автогенератора для детектирования попыток несанкционированного доступа к устройствам информационной безопасности

В статье рассматривается возможность использования LC-автогенератора в качестве чувствительного аппаратного датчика для обнаружения физических попыток несанкционированного доступа (НСД) к устройствам информационной безопасности. Предложена схема генератора на биполярном транзисторе по типу ёмкостной трёхточки (Колпитца). Выполнено моделирование в среде Micro-Cap, показавшее, что добавление паразитной ёмкости 10 пФ (имитация вмешательства) вызывает изменение частоты генерации на 50 кГц (относительное изменение ~2,2 %). Полученные результаты подтверждают принципиальную возможность построения простого и эффективного датчика НСД.

Ключевые слова: LC-автогенератор, ёмкостная трёхточка, Micro-Cap, несанкционированный доступ, паразитная ёмкость, датчик вмешательства, частота генерации.

Современные устройства информационной безопасности защищаются в основном программными средствами. Однако злоумышленник может воздействовать на устройство физически: вскрыть корпус, подключить дополнительный провод, изменить параметры кабеля или попытаться подключить стороннее устройство. Такие действия не всегда обнаруживаются обычными средствами контроля. Поэтому возникает задача создания простого и чувствительного аппаратного датчика, который будет реагировать на любое вмешательство. В качестве такого датчика предлагается использовать LC-автогенератор, поскольку его частота зависит от параметров колебательного контура. Даже небольшое изменение ёмкости или индуктивности приводит к изменению частоты, а значит, может быть зафиксировано как попытка НСД.

Цель работы – разработать и смоделировать LC-автогенератор, способный фиксировать изменение параметров колебательного контура при попытке несанкционированного доступа к устройству информационной безопасности. Задачи: рассмотреть принцип работы LC-автогенератора; разработать электрическую схему (ёмкостная трёхточка); выполнить моделирование в Micro-Cap; исследовать изменение частоты при добавлении паразитной ёмкости; сделать вывод о применимости схемы для обнаружения НСД.

LC-автогенератор – это электронное устройство, генерирующее незатухающие гармонические колебания[114]. Его основу составляет колебательный контур из катушки индуктивности L и конденсатора C. Частота собственных колебаний определяется формулой Томсона:

$$f_0 = \frac{1}{2\pi\sqrt{LC}}$$

В реальном контуре присутствуют потери, поэтому для поддержания колебаний используется активный элемент (транзистор) и положительная обратная связь[115]. В данной работе выбрана схема

[114] Кагарманов А. Р., Исупов Р. С. Исследование LC-автогенератора гармонических колебаний // Обеспечение информационной безопасности в электроэнергетике: современность и перспективы : сб. ст. Всерос. студ. науч.-практ. конф. с междунар. участием, Ижевск, 24 апреля 2025 года. Ижевск : Удмуртский университет, 2025. С. 61–65.

[115] Гоноровский И. С. Радиотехнические цепи и сигналы. М., 1986. С. 156–158.

ёмкостной трёхточки (Колпитца), так как она обеспечивает хорошую стабильность частоты и чувствительность к изменению ёмкости[116]. При нормальной работе параметры L и C постоянны, частота фиксирована. При физическом вмешательстве (вскрытие корпуса, приближение руки или металлического предмета, подключение дополнительного провода) возникает паразитная ёмкость, которая изменяет эквивалентную ёмкость контура, а следовательно, и частоту генерации. Именно это изменение предлагается использовать в качестве признака НСД.

Для моделирования в Micro-Cap использована схема LC-автогенератора на биполярном транзисторе BC547. Элементы схемы: транзистор VT1 – BC547; резисторы R1 = 47 кОм, R2 = 10 кОм, R3 = 1 кОм; конденсаторы C1 = 100 пФ, C2 = 100 пФ, C3 = 10 нФ (блокировочный); катушка индуктивности L1 = 100 мкГн; источник питания Vcc = 9 В. Колебательный контур образован элементами L1, C1, C2. Эквивалентная ёмкость контура:

$$C = \frac{C1 * C2}{C1 + C2} = \frac{100 * 100}{100 + 100} = 50\text{пФ}$$

Расчётная частота генерации в нормальном режиме:

$$f_1 = \frac{1}{2\pi\sqrt{L1 * C_{\text{экв}}}} = \frac{1}{2\pi\sqrt{100 * 10^{-6} * 50 * 10^{-12}}} = 2.25\text{МГц}$$

Результаты моделирования нормального режима представлены на рис. 1. На рис. 1 видно, что сигнал имеет форму, близкую к синусоидальной, частота устойчива и соответствует расчётной ~2,25 МГц.

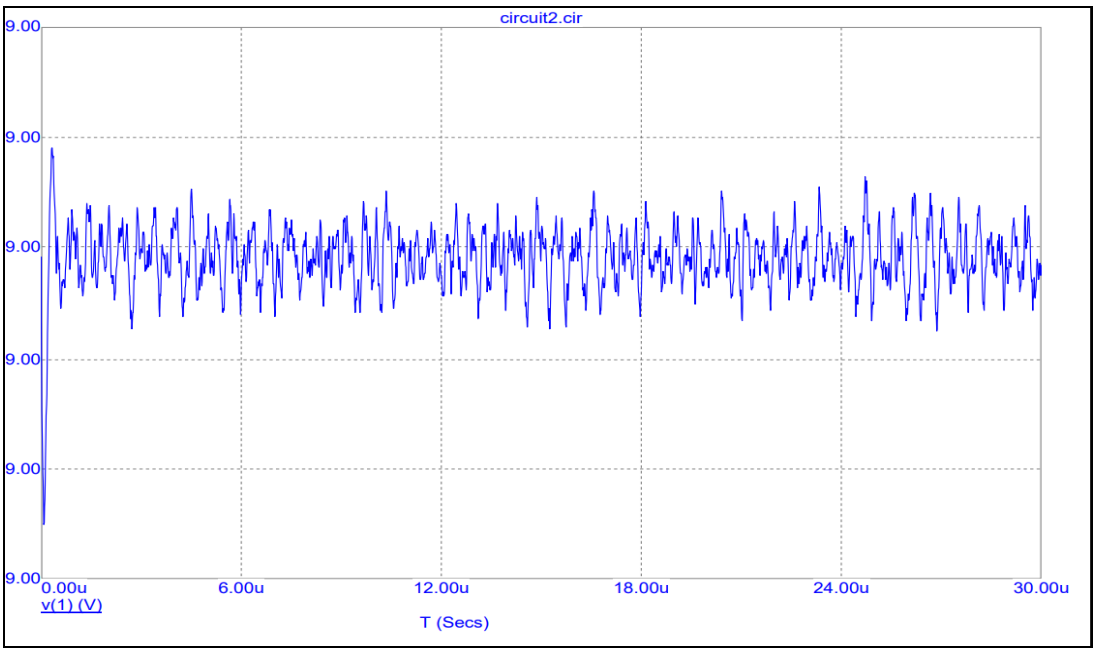


Рис. 1. График выходного сигнала в нормальном режиме

Для имитации несанкционированного доступа в схему добавлен дополнительный конденсатор C4 = 10 пФ, подключённый параллельно C2 (между базой и землёй). Это моделирует появление паразитной ёмкости при вмешательстве. Новое значение ёмкости C2' = 100 + 10 = 110 пФ. Эквивалентная ёмкость контура:

$$C_{\text{экв}} = \frac{100 * 100}{100 + 110} = 52.4\text{пФ}$$

Частота после добавления паразитной ёмкости:

$$f_2 = \frac{1}{2\pi\sqrt{100 * 10^{-6} * 52.4 * 10^{-12}}} = 2.20\text{МГц}$$

Изменение частоты $\Delta f = 2.25 - 2.20 = 0.05$ МГц $= 50$ кГц. Относительное изменение $\delta = \frac{50}{2250} * 100\% \approx 2.2\%$.

[116] Гусев В. Г., Гусев Ю. М. Электроника и микропроцессорная техника : учеб. для вузов. 3-е изд. перераб. и доп. М. : Высш. шк., 2004. С. 658–660.

В программе Micro-Cap выполнен временной анализ (Transient Analysis) с параметрами: время моделирования 50 мкс, шаг интегрирования 0,01 мкс, измеряемая точка – напряжение на коллекторе транзистора. Сначала проведено моделирование для нормального режима (без C4). Сигнал имеет форму, близкую к синусоидальной, частота устойчива и соответствует расчётной ~2,25 МГц. Затем в схему добавлен конденсатор C4 = 10 пФ (имитация НСД). Частота генерации снижается до ~2,20 МГц, период колебаний увеличивается. График выходного сигнала после имитации несанкционированного доступа приведён на рис. 2. Видно, что частота генерации снижается до ~2,20 МГц, период колебаний увеличивается. Основные результаты моделирования для двух режимов сведены в табл. 1.

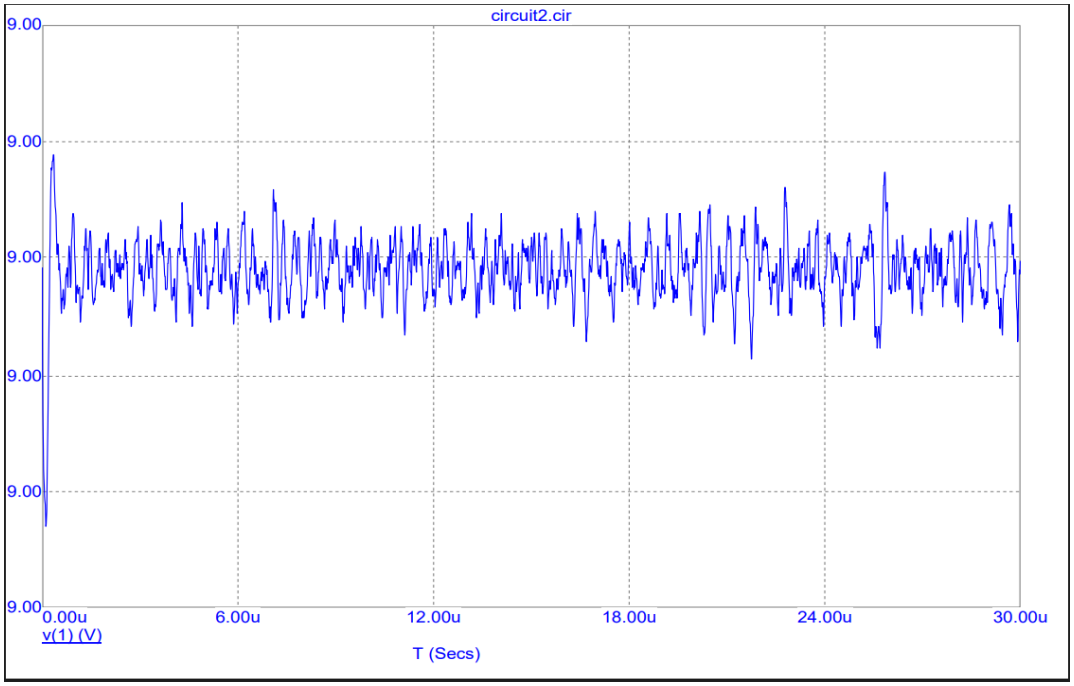


Рис. 2. График после имитации несанкционированного доступа

Таблица 1

Сравнение параметров генератора в нормальном режиме и после имитации

Параметр	Нормальный режим	После НСД (добавлена паразитная ёмкость 10 пФ)	Как проявляется влияние НСД
Ёмкость C2	100 пФ	110 пФ	При вмешательстве появляется дополнительная паразитная ёмкость от провода, руки или металлического предмета
Эквивалентная ёмкость контура	50 пФ	52.4 пФ	Общая ёмкость LC-контура возрастает
Индуктивность L1	100 мкГн	100 мкГн	Не изменяется, так как вмешательство влияет в первую очередь на электрическое поле
Частота генерации	2.25 МГц	2.20 МГц	Частота уменьшается на 50 кГц
Период колебаний	0.444 мкс	0.455 мкс	Период увеличивается, пики сигнала становятся дальше друг от друга
Изменение периода	—	+0.011 мкс	Увеличение периода хорошо видно на графике
Относительное изменение частоты	—	−2.2 %	Даже небольшое вмешательство вызывает измеримое изменение
Амплитуда сигнала	1.8–2.0 В	1.6–1.8 В	Возможна небольшая потеря амплитуды из-за изменения режима генерации
Форма сигнала	Стабильная, почти синусоидальная	Сохраняется, но становится менее устойчивой	При сильном вмешательстве возможны искажения
Положение максимумов на графике	Через каждые 0.444 мкс	Через каждые 0.455 мкс	На сравнительном графике пики второго сигнала постепенно смещаются вправо
Накопленное смещение через 10 периодов	0 мкс	≈ 0.11 мкс	Через несколько колебаний разница становится визуально заметной
Возможность обнаружения	Отсутствует тревога	Формируется сигнал тревоги	Если изменение частоты превышает установленный порог, система фиксирует НСД

В ходе работы был рассмотрен принцип действия LC-автогенератора и предложена схема его применения для обнаружения несанкционированного доступа к устройствам информационной безопасности. Моделирование в программе Micro-Cap показало, что даже небольшое изменение параметров колебательного контура (добавление паразитной ёмкости 10 пФ) приводит к заметному изменению частоты генерации – на 50 кГц (около 2,2 %). Такое изменение легко регистрируется простыми частотными детекторами, что позволяет использовать предложенную схему в качестве недорогого и эффективного аппаратного датчика вмешательства. Преимуществом подхода является высокая чувствительность к изменениям электрического поля, возникающим при большинстве физических воздействий на устройство. Дальнейшее развитие работы может включать разработку порогового устройства (компаратора или микроконтроллерного частотомера) для автоматической генерации сигнала тревоги, а также исследование влияния различных типов вмешательств (изменение индуктивности, внесение ферромагнетиков).

УДК 343.13:62:004(045)

Г. А. Касаткин,
обучающийся 4 курса Института права,
социального управления и безопасности ФГБОУ ВО «УдГУ».
Научный руководитель: Ф. А. Абашева, канд. юрид. наук, доцент
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Особенности применения отдельных технических средств и цифровых технологий при производстве следственных действий

Использование цифровых технологий и специализированных технических устройств проникло во все сферы жизнедеятельности и стало обыденным. Государство так же активно внедряет их в работу своих институтов, стремясь упростить процедуры и повысить эффективность. Эта практика затронула и сферу досудебного производства.

Сегодня следственная практика всё активнее осваивает технические средства и цифровые технологии – комплексы видеофиксации, биометрическую идентификацию, нейросетевые алгоритмы анализа данных, что позволяет раскрывать преступления. В частности, на полях XIII Петербургского международного юридического форума Председатель Следственного комитета РФ А. И. Бастрыкин сообщил, что: алгоритмы искусственного интеллекта (далее – ИИ) помогли раскрыть убийства политолога Дарьи Дугиной и военкора Владлена Татарского (Максима Фомина)[117].

Эти технологии повышают точность и объективность следственных действий, снижают человеческий фактор и минимизируют вероятность ошибок.

Постановка вопроса о применении технических средств не нова: в ч. 6 ст. 164 УПК РФ закреплено, что «при производстве следственных действий могут применяться технические средства и способы обнаружения, фиксации и изъятия следов преступления и вещественных доказательств»[118]. Так, ч. 2 ст. 166 УПК РФ обязывает указывать в протоколе применённые технические средства, а ст. 170 УПК РФ – обязательную видеофиксацию в случае производства следственного действия без участия понятых. Однако отсутствие единого законодательного понятия технических средств и цифровых технологий, процедур их применения, правоприменитель вынужден действовать в условиях нормативной неопределённости. Это порождает неоднородную практику. Как справедливо отмечает А. Ю. Чурикова, «зачастую подозреваемым необоснованно отказывают в использовании технических устройств, что приводит к ограничению их законных прав»[119].

Особую сложность представляют ситуации, где средства служат не вспомогательным инструментом фиксации, а способом получения сведений, имеющих самостоятельное значение для установления обстоятельств, указанных в ст. 73 УПК РФ.

---

[117] Бастрыкин А. И. Выступление на XIII Петербургском международном юридическом форуме (май 2025 г.) // Коммерсантъ. 2025. 19 мая. URL: https://www.kommersant.ru/doc/7735495 (дата обращения: 15.04.2026).

[118] Уголовно-процессуальный кодекс Российской Федерации : Федеральный закон от 18.12.2001 № 174-ФЗ (ред. от 31.07.2025) // СПС «КонсультантПлюс» (дата обращения: 15.04.2026).

[119] Чурикова А. Ю. Практика и проблемы регулирования использования технических средств в уголовном процессе // Российский судья. 2025. № 4. С. 56–60.

Соответственно, в статье будут рассмотрены конкретные особенности применения таких средств и возникающие при это практические нюансы.

Наиболее распространёнными остаются средства аудио- и видеофиксации: фотоаппараты, диктофоны, видеокамеры. О том, что они разрешены, упоминало выше, применительно к ст. 166 и 170 УПК. Однако при их использовании существует ряд нюансов.

Первое – процессуальный аспект. Согласно ч. 6 ст. 164 УПК РФ: «перед началом следственного действия следователь предупреждает лиц, участвующих в следственном действии, о применении технических средств». Если уведомление было сделано после начала записи или проигнорировано, то это может служить основанием для признания материалов недопустимыми доказательствами по п.п. 3 ч. 2 ст. 75 УПК РФ. В случае подачи ходатайства в рамках ст. 119–122 УПК РФ следователю, или же в прокуратуру по ст. 124 УПК РФ на стадии досудебного производства, это может быть расценено как существенное нарушение закона, влекущее ущемление прав участников.

Вторая особенность – соблюдение процедуры при отсутствии понятых. Согласно ч. 1.1 ст. 170 УПК РФ, если следственное действие проводится без них, применение технических средств фиксации обязательно. Показательным является Определение Шестого кассационного суда общей юрисдикции от 5 июля 2024 № 77-1974/2024[120]: следователь проводил осмотр АЗС без участия понятых. Суд кассационной инстанции установил, что на снимках запечатлен лишь общий вид АЗС, тогда как значимые для дела расстояния (от ТРК до операторной, до автодороги), которые легли в основу экспертных заключений, не были зафиксированы ни фотосъёмкой, ни иными техническими средствами. Это лишило суд возможности объективно оценить результаты осмотра. В итоге протокол признан недопустимым доказательством, а приговор отменён с направлением дела на новое рассмотрение. Данный случай демонстрирует: наличие фото и видеофиксации не гарантирует допустимость доказательства, если не обеспечена фиксация всех юридически значимых обстоятельств.

Следующая форма – дистанционное проведение следственных действий с помощью систем видео-конференц-связи. Данный механизм призван сократить время и снизить нагрузку на органы предварительного следствия. Законодательное он был закреплен лишь в конце 2021 года с введением в УПК ст. 189.1, позволившей проводить допрос, очную ставку посредством систем ВКС. Однако новизна темы, порождает множество нюансов.

Ключевая особенность – непосредственный канал связи. В п. 1 ст. 189.1 сказано, что использование ВКС допускается только при наличии технической возможности на обеих сторонах, что не всегда возможно реализовать: из-за недостаточной технической оснащённости или же по иным причинам.

Также отметим, что наличие технической возможности не гарантирует использование сертифицированных защищённых каналов связи, одобренных со стороны соответствующих органов. Использование иного ПО фактически запрещено в связи с «Указом Президента о запрете зарубежного программного обеспечения в критической информационной инфраструктуре», куда можно отнести ВКС[121]. Поэтому сотрудники лишены возможности реализовать предоставленное право. Нарушение этого требования влечёт последствия: суды последовательно признают протоколы, составленные по результатам допросов и очных ставок, проведённых через обычные приложения, недопустимыми доказательствами. Так, апелляционное определение Саратовского областного суда от 05.10.2023 по делу № 22-2582/2023 признаны недопустимыми протоколы очных ставок, проведённых не с помощью ВКС, а через программу «Movavi» и приложение «Viber»[122].

Требование ч. 4 ст. 189.1 УПК РФ вести видеозапись всего хода следственного действия и приобщать её к протоколу. Его несоблюдение влечёт признание протокола недопустимым доказательством. Существенным является обстоятельство, что в случае проведения следственного действия с помощью ВКС, часть процессуальных обязанностей ложится на следователя, обеспечивающего явку. Он должен проверить документы, разъяснить права и обязанности, взять подписку. Иначе протокол не будет допустимым.

В отличие от технических средств, давно известных и получивших примерные рамки использования, цифровые инструменты стали активно внедряться лишь в последние годы. Это технологии нового поколения, под которые ни у одного государства в полной мере не заточены ни законодательные, ни практические механизмы. Поэтому здесь особенности проявляются крайне остро.

---

[120] Определение Шестого кассационного суда общей юрисдикции от 05.07.2024 № 77-1974/2024 // СПС «КонсультантПлюс» (дата обращения: 15.04.2026).

[121] О дополнительных мерах по обеспечению информационной безопасности Российской Федерации : Указ Президента РФ от 01.05.2022 № 250 // СЗ РФ. 2022. № 19. Ст. 3195.URL: http://www.kremlin.ru/acts/bank/47796 (дата обращения: 16.04.2026).

[122] Апелляционное определение Саратовского областного суда от 05.10.2023 по делу № 22-2582/2023 // Судебные и нормативные акты РФ (СудАкт). URL: https://sudact.ru/regular/doc/ScaDVCp1bQJp/ (дата обращения: 17.04.2026).

К ним относятся: программные комплексы для извлечения и анализа данных, алгоритмы распознавания лиц, системы биометрической идентификации. Они работают в нефизическом пространстве и воспринимаются только через специальные устройства.

Первая особенность касается ИИ. 15 января 2026 года Председатель СК РФ Александр Бастрыкин в интервью ТАСС сообщал: «Что касается искусственного интеллекта, есть определенные наработки по его применению для выявления определенных закономерностей преступного поведения на основе анализа вводимых данных из материалов уголовных дел»[123]. Законодательное регулирование этих вопросов отсутствует.

Вторая особенность – биометрическая идентификация. Ключевая проблема – отсутствие в УПК РФ норм, регламентирующих сбор, хранение и использования биометрических данных при следственных действий. Это создаёт неопределённость: можно ли использовать данные распознавания лица как основание для задержания, как оформить идентификацию по голосу или отпечаткам пальцев через мобильное приложение. Действующее законодательство ответов не даёт.

Третья особенность связана с тем, что даже после сделанного шага вперёд – законопроект «О внесении изменений в отдельные законодательные акты Российской Федерации», одобренным 7 апреля 2026 года, – следователь остаётся в ситуации правовой неопределённости[124]. Новые нормы позволят направлять документы в электронном виде, но не затрагивают порядок производства следственных действий.

Последний рассматриваемый компонент: приостановление операций с денежными средствами. С 1 сентября 2025 года вступили в силу ФЗ № 278-280, предоставившие следователю и дознавателю новые полномочия – приостанавливать такие операции на срок до 10 суток[125].

Первая – это внесудебный характер: приостановление производится без предварительного судебного решения, что обусловлено необходимостью оперативного реагирования на киберпреступления.

Вторая – строго ограниченный срок (не более 10 суток). Он является предельным: с одной стороны, это даёт следователю время для получения судебного решения об аресте, а с другой – выступает гарантией от неограниченного по времени удержания средств без судебного контроля.

Третья – обязательное процессуальное согласование: постановление выносится следователем исключительно с согласия руководителя следственного органа, а дознавателем – с согласия прокурора, что в целом минимизирует риск необоснованного применения.

Проведённое исследование демонстрирует, что применение цифровых технологий и технических средств при производстве следственных действий характеризуется некой нормативной фрагментарностью и отсутствием системного регулирования. И даже когда законодатель прямо допускает использование тех или иных устройств, детальный порядок их применения остаётся неурегулированным, а судебная практика демонстрирует не единообразие в оценке допустимости доказательств.

Для аудио- и видеофиксации на первый план выходят предупреждение участников и полнота фиксации значимых обстоятельств при отсутствии понятых. Для ВКС – это жёсткие требования к каналу связи и коллизией с запретом зарубежного ПО в критической инфраструктуре. ИИ и биометрия на сегодняшний день вообще внедряются без специальных процессуальных норм. Новеллы 2025 г. о блокировке счетов, содержат оценочные основания, требующие внимания правоприменителя.

Резюмируя, отметим, что дальнейшее развитие законодательства должно развиваться не по пути точечных поправок, а формирования конкретизированного системного подхода, включающего как легальные определения, единые требования к сертификации и оформлению результатов, так и гарантии прав участников судопроизводства.

---

[123] Бастрыкин А. И. Интервью ТАСС 15 января 2026 г. // ТАСС. 2026. URL: https://tass.ru/ekonomika/26153047 (дата обращения: 18.04.2026).

[124] Комиссия правительства одобрила законопроект об электронных приговорах по уголовным делам // Право.ru. 2026. 7 апреля. URL: https://pravo.ru/news/259335/ (дата обращения: 22.05.2026).

[125] О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации : Федеральный закон от 31.07.2025 № 278-ФЗ // СЗ РФ. 2025. № 31. Ст. 5210; О внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 31.07.2025 № 279-ФЗ // Там же. 2025. № 31. Ст. 5211; О внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 31.07.2025 № 280-ФЗ // Там же. 2025. № 31. Ст. 5212.

УДК 519.246:378:004(045)

И. А. Князев,
обучающийся 2 курса Института права,
социального управления и безопасности ФГБОУ ВО «УдГУ».
Научный руководитель: М. М. Гайсин, старший преподаватель
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Анализ временных рядов

В современных условиях цифровизации науки и образования статистический анализ данных приобретает всё большее значение. Специалисты в области информационной безопасности, анализа данных, математического моделирования регулярно сталкиваются с задачами описательной статистики, проверки статистических гипотез и визуализации данных. Вместе с тем, существующие инструменты зачастую либо чрезмерно сложны для начинающих пользователей, либо лишены интерактивности и наглядности, необходимых в учебном процессе.

В связи с этим актуальной задачей является разработка программного обеспечения, которое сочетает в себе доступный интерфейс, широкие аналитические возможности и образовательный потенциал. Настоящая статья посвящена описанию архитектуры, реализации и функциональности приложения MathLab PRO – оригинального программного продукта, разработанного на языке Python 3.8+ и предназначенного для студентов, исследователей и специалистов в области статистики и теории вероятностей.

Цель исследования - описание принципов проектирования и реализации многофункционального инструмента статистического анализа, включающего визуализацию вероятностных распределений, анализ временных рядов, сравнение выборок и обучающий игровой модуль.

*Материалы и методы***.** Вероятностное распределение – это математическая функция, описывающая вероятность принятия случайной величиной тех или иных значений. Распределения лежат в основе математической статистики, теории принятия решений и машинного обучения. Наиболее важные из них с точки зрения практического применения в области информационной безопасности и анализа данных включают: нормальное, экспоненциальное, Пуассона, биномиальное, равномерное, логнормальное и бета-распределение[126].

Нормальное распределение (распределение Гаусса) описывается плотностью вероятности $f(x) = (1 / (\sigma\sqrt{(2\pi)})) \cdot \exp(-0{,}5 \cdot ((x - \mu) / \sigma)^2)$, где μ – математическое ожидание, σ – стандартное отклонение. Оно является наиболее распространённым в природе и играет центральную роль в статистике в силу центральной предельной теоремы. Распределение Пуассона $P(X = k) = (e^{(-\mu)} \cdot \mu^k) / k!$ применяется при моделировании редких событий – например числа сетевых инцидентов за единицу времени. Экспоненциальное распределение $f(x) = \lambda \cdot e^{(-\lambda x)}$ описывает время между событиями и широко используется в теории надёжности[127].

Язык Python является одним из наиболее популярных в научном программировании благодаря богатой экосистеме библиотек. Для задач численных вычислений и работы с матрицами используется NumPy, для статистической обработки сигналов и расчёта критериев – SciPy, для построения графиков – Matplotlib. В качестве фреймворка для создания графического интерфейса в MathLab PRO используется ttkbootstrap – современная надстройка над Tkinter, предоставляющая темизируемые виджеты в стиле Bootstrap 5[128].

Среди аналогов описываемого продукта можно выделить SPSS, Stata и R Studio. Однако эти инструменты ориентированы на профессионалов и требуют значительного времени на освоение. Python-приложение MathLab PRO занимает нишу интерактивного образовательного инструмента, доступного для пользователя с базовым уровнем технической подготовки.

Результаты и обсуждения. Архитектура MathLab PRO реализована по принципу однофайлового монолитного приложения с разделением логики по классам. Приложение написано на Python 3.8+ и организовано по паттерну MVC (Model-View-Controller) в упрощённом варианте: каждая вкладка представляет собой отдельный класс-контроллер (DistributionFrame, CorrelationFrame, CompareFrame,

[126] Гмурман В. Е. Теория вероятностей и математическая статистика : учеб. пособие. М. : Высш. школа, 2003. С. 479.
[127] Боровков А. А. Математическая статистика. М. : Наука, 2010. С. 704.
[128] Боровков А. А. Математическая статистика. М. : Наука, 2010. С. 704.

GameFrame, MegaHelpFrame), инкапсулирующий как логику обработки данных, так и элементы пользовательского интерфейса. Главный класс App наследуется от tb.Window и управляет компоновкой всех модулей через объект MainArea.

Приложение запускается функцией main() и создаёт единственный экземпляр класса App. Боковая панель (Sidebar) содержит навигационные кнопки, верхняя панель (Topbar) отображает название и системное время, основная область (MainArea) хранит фреймы вкладок и переключает их по команде. Данные о рекордах пользователя сохраняются в локальный JSON-файл в директории ~/.mathlab_pro.

Основные зависимости приложения: NumPy (вычисления с многомерными массивами), SciPy (функции статистического анализа: ttest_ind, ks_2samp, gaussian_kde, signal.savgol_filter, gaussian_filter1d), Matplotlib (рендеринг графиков через FigureCanvasTkAgg), ttkbootstrap (интерфейс). Дополнительно подключается библиотека Pandas для чтения файлов форматов XLSX и XLS. Все зависимости проверяются при запуске с информативными сообщениями об ошибке; отсутствие Pandas не является критическим и обрабатывается через флаг PANDAS_AVAILABLE.

Тема интерфейса – Flatly. Используются три фирменных цвета: основной (#357EDD – синий), вторичный (#2ECC71 – зелёный) и сигнальный (#E74C3C – красный). Разрешение окна составляет 1360×820 пикселей. Размер программы в машиночитаемой форме – 82 990 байт.

Вкладка «Распределения» является центральным модулем приложения. Пользователь выбирает одно из семи поддерживаемых распределений (равномерное, нормальное, экспоненциальное, Пуассона, биномиальное, логнормальное, бета), задаёт его параметры и размер выборки от 1 до 100 000 точек. По нажатию кнопки «Генерировать» вычисляется выборка с помощью генераторов NumPy, после чего строится гистограмма с наложенной кривой ядерной оценки плотности (KDE), реализованной через scipy.stats.gaussian_kde.

Предусмотрена возможность импорта данных из файлов CSV, TXT, XLSX и XLS. Поддерживаются три метода сглаживания графиков: фильтр Савицкого-Голея (scipy.signal.savgol_filter), гауссово размытие (scipy.ndimage.gaussian_filter1d) и скользящее среднее (rolling mean на основе NumPy). Это позволяет работать как с синтетическими, так и с реальными наборами данных, сравнивая теоретические распределения с эмпирическими.

Вкладка «Автокорреляция (ACF)» реализует визуализацию функции автокорреляции временного ряда. Пользователь задаёт максимальное число лагов и опционально применяет предварительное сглаживание исходных данных. Вычисление ACF выполняется по стандартной формуле с нормализацией и отображается в виде столбчатой диаграммы с горизонтальными доверительными границами $\pm 1{,}96/\sqrt{n}$. Данный инструмент позволяет выявлять периодические компоненты, сезонность и структуру зависимостей в последовательных наблюдениях[129].

Вкладка «Сравнение» предназначена для сопоставления двух независимых выборок данных с использованием непараметрических и параметрических критериев. Реализованы критерий Стьюдента (scipy.stats.ttest_ind) для проверки гипотезы о равенстве математических ожиданий и критерий Колмогорова-Смирнова (scipy.stats.ks_2samp) для проверки гипотезы об однородности распределений. Результаты выводятся в числовом виде (статистика теста и p-value) с интерпретацией на уровне значимости 0,05, а также визуализируются в виде совмещённых гистограмм KDE.

Модуль MathMaster представляет собой оригинальную интерактивную обучающую игру, разработанную с целью закрепления знаний по математике и теории вероятностей. Предусмотрены четыре режима: арифметические операции (вычисление выражений), сравнение пар выражений, поиск арифметических ошибок и викторина по свойствам распределений. Каждый режим поддерживает три уровня сложности (Easy, Medium, Hard), определяющих диапазоны операндов.

Игровая сессия ограничена таймером (настраиваемый интервал). За правильный ответ начисляются очки (10 за арифметику, 12 за поиск ошибок, 15 за сравнение, 20 за викторину по распределениям). По завершении сессии результат сравнивается с рекордом, хранящимся в локальном JSON-файле; при установлении нового рекорда выводится соответствующее уведомление. Такой подход к геймификации способствует мотивации и самоконтролю учащихся.

С точки зрения информационной безопасности приложение MathLab PRO может рассматриваться в двух плоскостях: как инструмент обучения основам статистики, применяемым в области ИБ, и как самостоятельный программный продукт, требующий анализа безопасности.

Во-первых, распределение Пуассона активно используется в IDS/IPS-системах для моделирования числа сетевых событий и выявления аномалий. Нормальное распределение лежит в основе методов машинного обучения для обнаружения вторжений. Экспоненциальное распределение применяется

[129] Лукацкий А. В. Обнаружение атак. СПб. : БХВ-Петербург, 2001. С. 624.

при оценке надёжности криптографических компонентов и времени до отказа. Таким образом, практические навыки работы с распределениями, формируемые при использовании MathLab PRO, непосредственно востребованы в профессиональной деятельности специалиста по информационной безопасности.

Во-вторых, рассмотрим непосредственную безопасность самого приложения. Все пользовательские данные хранятся локально в директории ~/.mathlab_pro в незашифрованном формате JSON. Для учебного приложения это допустимо, однако при промышленном использовании следует рассмотреть шифрование локального хранилища. Загрузка внешних файлов данных осуществляется без валидации содержимого на предмет вредоносных данных (например, formula injection в CSV), что является рекомендуемой областью улучшения. Приложение не взаимодействует с сетью и не содержит серверных компонентов, что существенно снижает поверхность атаки.

В ходе разработки MathLab PRO была создана полнофункциональная кроссплатформенная десктопная программа, работающая под управлением Windows, macOS и Linux. Объём исходного кода составил порядка 1200 строк на языке Python, размер дистрибутива в машиночитаемой форме – 82 990 байт. Реализованы пять основных модулей, охватывающих задачи генерации и визуализации распределений, анализа временных рядов, статистического сравнения выборок и обучающей игры.

Использование библиотек NumPy, SciPy и Matplotlib обеспечило высокую точность вычислений и производительность при работе с выборками до 100 000 точек. Применение ttkbootstrap позволило создать современный пользовательский интерфейс без использования тяжёлых фреймворков, сохранив компактность приложения. Архитектурное решение в виде монолитного класс-ориентированного приложения обеспечивает простоту сопровождения и расширения кода.

Образовательный модуль MathMaster представляет собой оригинальный вклад в функциональность продукта и выгодно отличает его от аналогичных инструментов. Геймификация обучения статистике и теории вероятностей способствует повышению вовлечённости студентов и закреплению теоретического материала.

В настоящей статье представлено описание архитектуры и функциональных возможностей программного приложения MathLab PRO, разработанного на языке Python с использованием библиотек NumPy, SciPy, Matplotlib и ttkbootstrap. Программа обеспечивает широкий спектр возможностей для статистического анализа и визуализации данных, включая работу с семью типами вероятностных распределений, анализ функции автокорреляции, сравнение двух выборок посредством параметрических и непараметрических критериев, а также интерактивный обучающий модуль.

Разработанный продукт может быть использован в учебном процессе по направлениям «Информационная безопасность», «Прикладная математика и информатика», «Анализ данных», а также в исследовательской практике для экспресс-анализа данных. Перспективами дальнейшего развития являются: добавление новых типов распределений и статистических тестов, реализация модуля регрессионного анализа, интеграция с облачным хранилищем данных и шифрование локальных файлов пользователя.

УДК 621.316.825:621.382.3(045)

И. А. Князев,
обучающийся 2 курса Института права,
социального управления и безопасности ФГБОУ ВО «УдГУ».
Научный руководитель: Т. Н. Стерхова, канд. техн. наук, доцент
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Исследовательские испытания светодиодного светильника, основанного на LDR резисторе

Светочувствительный ночник на фоторезисторе (LDR) и одном транзисторе представляет собой простейшее автоматическое устройство, которое включает светодиод при уменьшении освещённости и отключает его при достаточном уровне света. В основе работы лежит изменение сопротивления LDR под действием света и использование биполярного транзистора в режиме ключа. Главные преимущества: один специализированный элемент (LDR), остальные – типовые простые компоненты, простая логика работы и хорошая наглядность физических процессов.

Цель исследования – экспериментально и теоретически проанализировать работу светочувствительного ночника на LDR и одном NPN-транзисторе, обосновать выбор элементной базы и параметров делителя, а также показать, как изменение сопротивления фоторезистора управляет включением светодиода через транзисторный ключ.

Материалы и методы предполагают минимальный набор компонентов: LDR (фоторезистор) общего назначения. В научных работах рассматриваются элементы с сопротивлением порядка единиц–десятков кОм при освещении и сотен кОм в темноте. Биполярный NPN-транзистор малой мощности BC547 или аналогичный (2N2222, 2N3904 и др.), пригодный для работы в режиме ключа при токах коллектора до нескольких десятков миллиампер. Резистор 470 Ом в цепи светодиода для ограничения тока. Один светодиод малой мощности (индикаторный). Источник питания 3 В (например, батарея 3 В)[130].

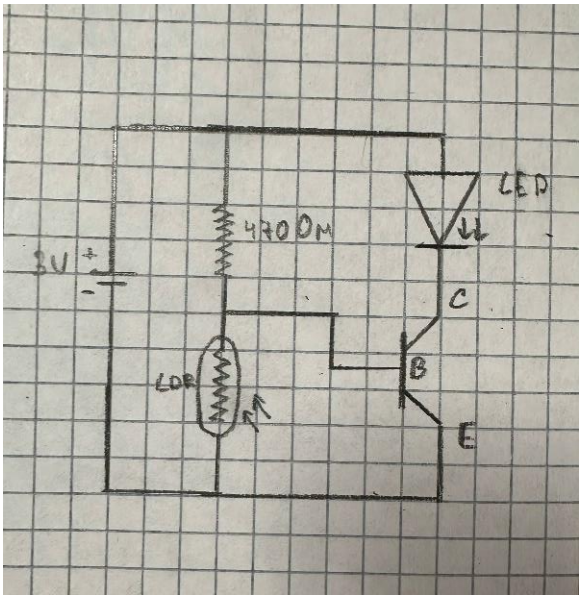
Результаты и обсуждения. Фоторезисторы относятся к фоточувствительным резистивным элементам, сопротивление которых уменьшается при увеличении освещённости. В методических материалах по исследованию характеристик LDR указывается, что сопротивление LDR в темноте достигает сотен кОм, а при освещении падает на порядок и более.

Физически изменение сопротивления связано с переходом электронов из валентной зоны в зону проводимости под действием фотонов: увеличение числа носителей заряда приводит к росту проводимости материала и уменьшению сопротивления.

Транзисторный ключ на NPN-транзисторе рассматривается как устройство, работающее в двух основных режимах: отсечка (закрытое состояние) и насыщение (открытое состояние). При напряжении база–эмиттер ниже примерно 0,6–0,7 В транзистор закрыт, ток коллектора пренебрежимо мал; при достаточном токе базы транзистор насыщается, и напряжение коллектор–эмиттер уменьшается до малой величины (десятые доли вольта), позволяя протекать току через нагрузку[131].

Снизу представлена типовую схема ночника с LDR и транзистором. Аналогичные схемы рассматриваются в статьях об автоматических ночниках и уличном освещении на LDR.

Это простая схема с датчиком света и светодиодом (рис. 1). Справа стоит фоторезистор (LDR), внизу – резистор, слева – светодиод.



- Фоторезистор справа включён в цепь управления.
- Резистор снизу ограничивает ток и задаёт режим работы.
- Светодиод слева служит нагрузкой/индикатором.
- Питание 3.7 V подаётся от аккумулятора, как подписано на изображении.

Рис. 1. Схема светочувствительного ночника на LDR

Схема, по компоновке, работает как светочувствительный выключатель или индикатор: при изменении освещённости сопротивление фоторезистора меняется, и это влияет на ток через светодиод. Такой узел часто используют в простых ночниках, автоподсветке и демонстрационных схемах.

Таким образом, LDR и резистор формируют сигнал управления (напряжение на базе), а транзистор и светодиод реализуют выходную ступень, включающую светодиод в темноте.

[130] Automatic night lamp using LDR // IRJET. Vol. 11, Issue 4. URL: https://www.ijera.com/papers/vol15no1/150197100.pdf (дата обращения: 24.04.2026).

[131] Automatic night lamp using LDR // IJERA Vol. 15, No. 1. URL: https://www.ijera.com/papers/vol15no1/150197100.pdf (дата обращения: 24.06.2026).

Согласно базовой теории делителя напряжения, напряжение на нижнем резисторе делителя определяется формулой:

$$V_{\text{база}} = V_{CC} \cdot \frac{R_{\text{пор}}}{R_{LDR} + R_{\text{пор}}}$$

где R_{LDR} – сопротивление фоторезистора, $R_{\text{пор}}$ – сопротивление резистора на землю. Из формулы видно: при уменьшении R_{LDR} (яркий свет) напряжение $V_{\text{база}}$ уменьшается; при увеличении R_{LDR} (темнота) $V_{\text{база}}$ возрастает и приближается к V_{CC}[132].

Используя экспериментально измеренную зависимость сопротивления LDR от освещённости, можно оценить напряжение на базе при разных уровнях освещения и таким образом оценить порог срабатывания схемы.

Транзистор открывается, когда напряжение на базе превышает примерно 0,6 В, и при дальнейшем росте переходит в режим насыщения. Следовательно, порог срабатывания можно описать неравенством:

$$V_{\text{база}} \geq V_{\text{пор}} \approx 0{,}6\text{–}0{,}7 \text{ В}$$

Подставляя выражение для $V_{\text{база}}$, получаем условие на отношение R_{LDR} и $R_{\text{пор}}$ при заданном V_{CC}. Это позволяет: подобрать номинал Rпор исходя из характерного сопротивления LDR при «граничной» освещённости; оценить, при каком уровне освещённости (в люксах) по экспериментальным данным LDR произойдёт включение ночника.

Эксперименты с LDR показывают, что при освещении сопротивление уменьшается до нескольких кОм. В этом режиме:

1. R_{LDR} мало по сравнению с $R_{\text{пор}}$, делитель «тянет» базовый узел к земле, и $V_{\text{база}}$ становится значительно меньше $V_{\text{пор}}$.
2. База транзистора не получает достаточного прямого смещения, транзистор находится в режиме отсечки, ток коллектора практически отсутствует.
3. Светодиод, включенный в цепи коллектора, не получает тока и остаётся погашенным.

С точки зрения потребления энергии в этом режиме ток ограничивается током через делитель LDR–Rпор, что учитывается при проектировании устройств с автономным питанием.

При отсутствии света сопротивление LDR увеличивается на порядок и более относительно освещённого состояния (см. рис. 2).

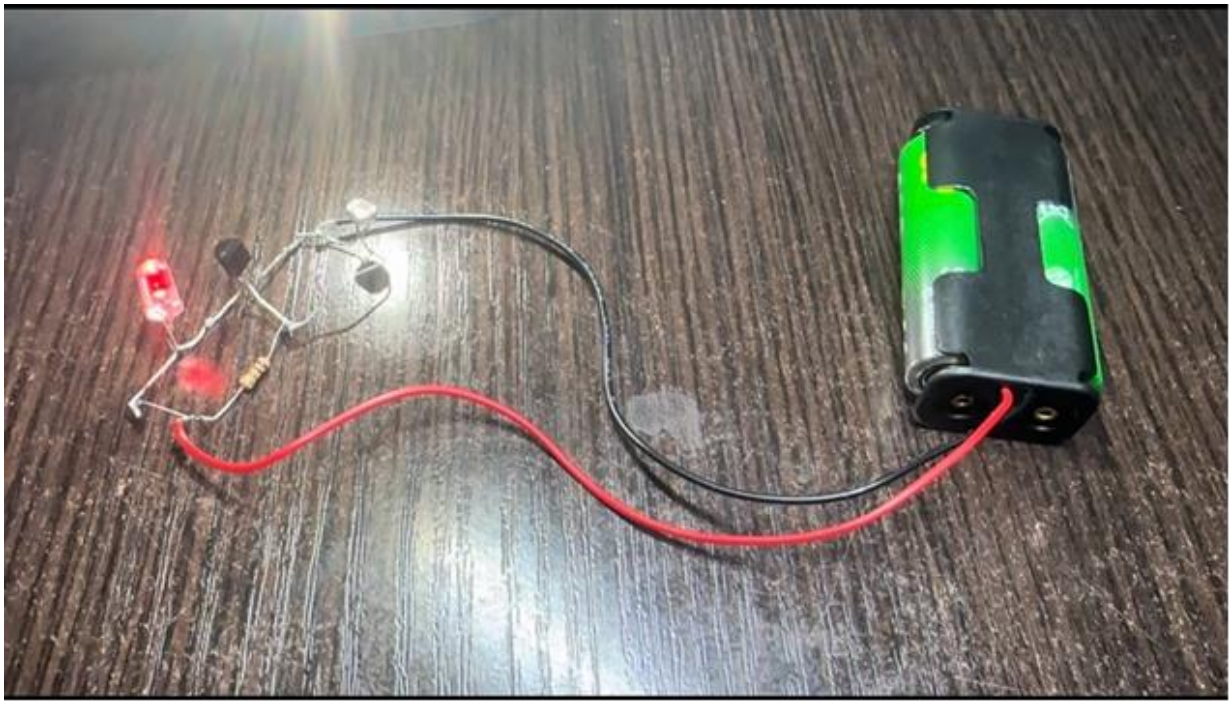


Рис. 2. Работа ночника при недостаточном освещении

[132] Automatic Street Light Using LDR // JNAO-NU. URL: https://www.instructables.com/Automatic-Street-Light-Using-Ldr/ (дата обращения: 25.06.2026).

В этом режиме:

1. R_{LDR} существенно превосходит $R_{\text{пор}}$, и делитель поднимает базовый узел к напряжению питания, обеспечивая $V_{\text{база}} \geq 0{,}6$ В.

2. База транзистора получает ток, транзистор открывается и при достаточном токе базы переходит в насыщение, что соответствует малому напряжению коллектор–эмиттер.

3. Через светодиод и резистор 470 Ом протекает ток, достаточный для свечения, при этом ток задаётся в основном резистором и падением напряжения на светодиоде.

Так реализуется автоматическое включение подсветки только при недостаточной освещённости, что подчёркивается как ключевое преимущество подобных схем.

Пример сборки светочувствительного ночника: разместить транзистор BC547 (или аналог) с эмиттером на общий провод; включить светодиод с резистором между шиной питания и коллектором; собрать делитель LDR–Rпор между шиной питания и землёй; подключить базу транзистора к узлу делителя и при необходимости добавить резистор база–эмиттер для надёжного закрытия. Также после сборки стоит проверить схему с помощью регулируемого источника света (лампа, свет от окна) и понаблюдать за включением/выключением светодиода (см. рис. 3).

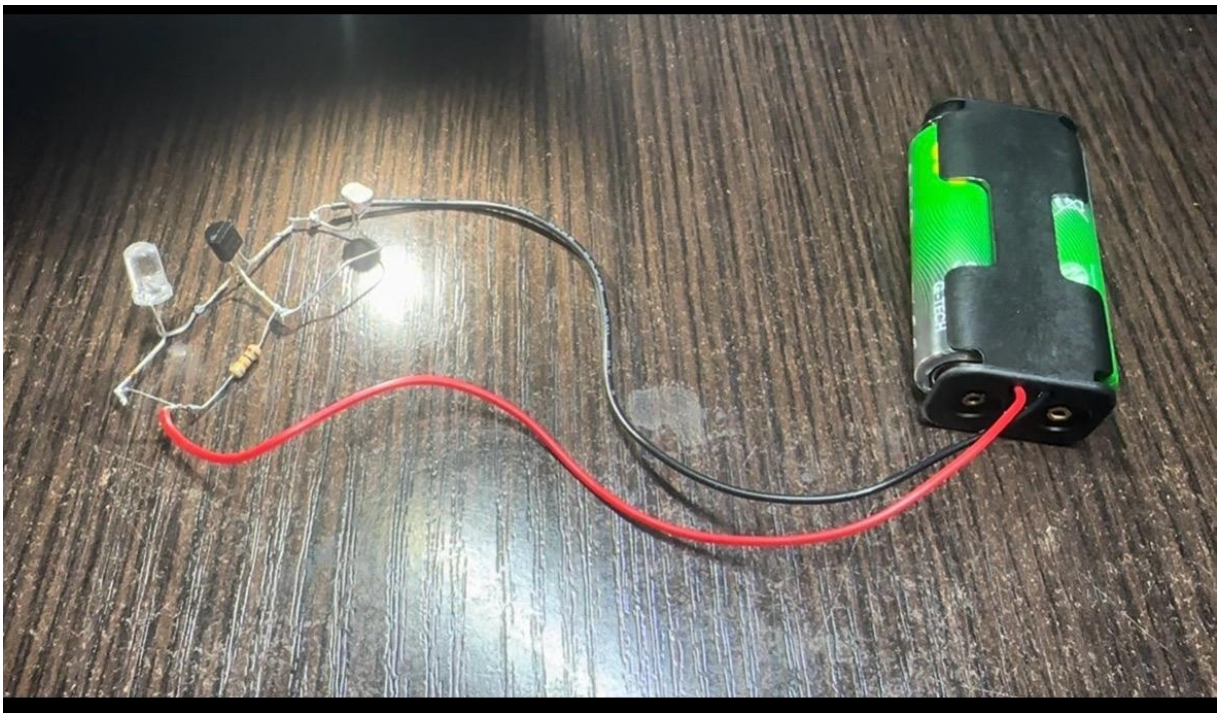


Рис. 3. Работа ночника при попадании света на фоторезистор

Для задания порога удобно применять подстроечный резистор (потенциометр). Следует изменять сопротивление Rпор и фиксировать уровни освещённости (или расстояние до источника света), при которых светодиод включается и выключается; построить зависимость порога срабатывания от номинала Rпор, сопоставляя экспериментальные данные с расчётом по формуле делителя.

Такое задание демонстрирует связь схемотехнических параметров (номиналы резисторов) с измеряемыми физическими величинами (освещённость).

В научных проектах отмечается, что при неподходящем выборе номиналов возможен режим, когда транзистор при «дне» не полностью закрыт, а светодиод слабо тлеет. Для устранения этого эффекта рекомендуют: уменьшить сопротивление Rпор; добавить резистор между базой и эмиттером для «подтяжки» базы к земле; подбирать LDR с более подходящими параметрами сопротивления в свету и темноте.

Простейший ночник, построенный только на делителе и одном транзисторе, имеет один порог включения и не обладает гистерезисом: при освещённости, близкой к пороговой, возможны частые переключения. В более продвинутых лабораторных работах предлагается: вводить положительную обратную связь (например, второй транзистор или операционный усилитель) для формирования гистерезиса; использовать RC-цепочки для сглаживания быстрых изменений освещения.

В результате исследования показано, что даже на основе минимальной элементной базы (LDR, один NPN-транзистор и несколько резисторов) можно построить надёжный светочувствительный

ночник, автоматически включающий светодиод при снижении освещённости и отключающий его при достаточном уровне света, что подтверждается теоретическим анализом делителя и транзисторного ключа, а также экспериментальным изучением режимов «день» и «ночь». Дополнительно установлено, что выбор номиналов резисторов в цепи делителя и наличие (или отсутствие) вспомогательных элементов (резистор база-эмиттер, подстроечный резистор) существенно влияет на порог срабатывания, качество выключения (отсутствие «подсвета») и устойчивость работы схемы, а учёт этих факторов позволяет целенаправленно настроить устройство под конкретные условия освещённости и демонстрирует практическую значимость простой транзисторной автоматики.

УДК 621.311:621.391.82:004.056(045)

А. С. Колчина,
обучающаяся 2 курса Института права,
социального управления и безопасности ФГБОУ ВО «УдГУ».
Научный руководитель: Т. Н. Стерхова, канд. техн. наук, доцент
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Влияние электромагнитных помех на системы управления электроэнергетическими объектами как фактор риска для информационной безопасности

Современная электроэнергетика представляет собой киберфизическую систему, в которой цифровые технологии управления неразрывно связаны с физическими процессами производства, передачи и распределения электроэнергии. В условиях цифровой трансформации энергетического сектора проблема защиты управляющих систем от дестабилизирующих факторов приобретает критическое значение для национальной безопасности. Одним из недостаточно изученных, но потенциально опасных векторов угроз выступают электромагнитные помехи, способные нарушить функционирование систем управления как непреднамеренно, так и в результате целенаправленных воздействий. Целью настоящего доклада является комплексный анализ влияния электромагнитных помех на системы управления электроэнергетическими объектами с позиции информационной безопасности и разработка рекомендаций по минимизации соответствующих рисков

1. Специфика современных систем управления электроэнергетическими объектами в контексте информационной безопасности

Современные АСУ ТП электростанций и подстанций представляют собой распределённые киберфизические комплексы, объединяющие устройства релейной защиты и автоматики (РЗА), системы телемеханики, средства учёта электроэнергии, устройства регистрации аварийных событий и системы видеонаблюдения. Архитектура таких систем строится на базе международных стандартов IEC 61850, определяющих протоколы обмена между интеллектуальными электронными устройствами через высокоскоростные промышленные сети Ethernet[133]. Использование единой сетевой инфраструктуры для передачи критически важной управляющей информации создаёт новые уязвимости, отсутствовавшие в эпоху аналоговых систем с жёсткой логикой.

Информационная безопасность энергетических объектов традиционно фокусировалась на защите от кибератак через цифровые каналы связи, вирусов, несанкционированного доступа, DDoS-атак. Однако физический уровень взаимодействия, где цифровые сигналы преобразуются в электрические импульсы и передаются по проводникам или в эфире, остается вне фокуса специалистов по информационной безопасности. Между тем на физическом уровне электромагнитные помехи способны вызвать искажение или полную потерю управляющей информации без какого-либо логического вмешательства в программное обеспечение. Микропроцессорные устройства, построенные на основе CMOS-технологий с напряжением питания 3,3–5 В и рабочими токами в милиамперах, обладают высокой чувствительностью к индуцированным напряжениям и токам[134].

[133] Аверьянов Е. В., Сердюков М. С. Электромагнитная совместимость устройств релейной защиты и автоматики в условиях грозовых воздействий // Электроэнергетика. Передача и распределение. 2022. № 4 (73). С. 32–39.

[134] Гизатуллин Ф. А., Закиров Р. М. Методы защиты микропроцессорных устройств РЗА от электромагнитных помех // Известия высших учебных заведений. Проблемы энергетики. 2022. Т. 24, № 3. С. 87–112.

Электромагнитный импульс достаточной мощности может вызвать ложное срабатывание логических элементов, повреждение полупроводниковых структур или полный выход из строя электронных компонентов.

2. Классификация источников электромагнитных помех как дестабилизирующих факторов киберфизических систем.

Электромагнитные помехи, воздействующие на системы управления электроэнергетическими объектами, характеризуются значительным разнообразием по природе возникновения, частотному спектру, мощности и механизмам проникновения в чувствительную аппаратуру.

В соответствии с международными стандартами электромагнитной совместимости и российскими нормативными документами целесообразно разделить источники помех на естественные и искусственные, причём последние подразделяются на непреднамеренные и преднамеренные[135].

Механизмы проникновения электромагнитных помех в системы управления включают кондуктивную связь через цепи питания и сигнальные кабели, индуктивную и емкостную связь с протяжёнными проводниками, а также прямое воздействие излучения на электронные компоненты. Наиболее опасными являются ситуации, когда несколько источников помех действуют одновременно, создавая сложную электромагнитную обстановку, превышающую проектные уровни помехоустойчивости оборудования.

3. Анализ механизмов воздействия электромагнитного излучения на микропроцессорную аппаратную базу.

Воздействие электромагнитного излучения приводит к индуцированию дополнительных токов и напряжений в проводниках печатных плат, корпусах микросхем и соединительных кабелях, что может вызвать ложное переключение логических элементов, нарушение синхронизации и потерю данных даже при сохранении физической целостности компонентов[136].

Низкочастотные электромагнитные поля промышленной частоты (50 Гц) и её гармоник, характерные для электроэнергетических объектов, воздействуют на аппаратуру преимущественно через магнитную составляющую, индуцируя токи в замкнутых контурах проводников. Согласно закону электромагнитной индукции Фарадея, изменяющийся магнитный поток через контур площадью S вызывает ЭДС, пропорциональную скорости изменения потока. Для типичных монтажных контуров систем вторичной коммутации площадью 0,1–1 м² магнитное поле напряжённостью 100 А/м на частоте 50 Гц индуцирует напряжения порядка единиц милливольт, что обычно недостаточно для нарушения работы цифровых устройств. Однако при наличии быстро изменяющихся процессов коммутации высоковольтного оборудования, коротких замыканий частотный спектр расширяется до десятков килогерц, что на несколько порядков увеличивает индуцированные напряжения и может привести к сбоям в работе микропроцессорных терминалов[137].

4. Технические методы защиты каналов связи и оборудования от преднамеренных электромагнитных воздействий.

Комплексная защита систем управления электроэнергетическими объектами от электромагнитных помех базируется на многоуровневом подходе, включающем меры на этапах проектирования, монтажа и эксплуатации оборудования.

Экранирование представляет наиболее эффективный метод защиты от электромагнитного излучения и основано на отражении и поглощении электромагнитной энергии металлическими оболочками. Эффективность экранирования (SE) измеряется в децибелах и определяется как отношение напряжённости поля без экрана к напряжённости поля с экраном.

Фильтрация помех в цепях питания и сигнальных линиях осуществляется с помощью пассивных LC-фильтров, варисторов и газоразрядных разрядников. Сетевые фильтры промышленного исполнения обеспечивают ослабление высокочастотных составляющих помех на 40–80 дБ в диапазоне от 150 кГц до 100 МГц при сохранении пропускания сигналов промышленной частоты. Варисторы на основе оксида цинка ограничивают амплитуду импульсных перенапряжений до безопасных уровней за счёт резкого уменьшения сопротивления при превышении порогового напряжения.

Система заземления выполняет двойную функцию: обеспечивает безопасность персонала при повреждении изоляции и создаёт эквипотенциальную поверхность для предотвращения протекания помеховых токов через чувствительное оборудование. Традиционное заземление на промышленной

---

[135] Кузнецов А. П., Миронова Т. В., Пастухов О. С. Классификация источников электромагнитных помех на объектах электроэнергетики // Электротехника. 2022. № 6. С. 43–49.

[136] Петров И. В., Соколов А. А. Нормативное обеспечение информационной безопасности объектов критической информационной инфраструктуры энергетики // Вестник кибербезопасности. 2023. № 1 (13). С. 200–207.

[137] Розанов М. Н. Требования технических регламентов к электромагнитной совместимости оборудования электроэнергетических объектов // Новое в российской электроэнергетике. 2022. № 7. С. 160–170.

частоте с сопротивлением растеканию менее 4 Ом оказывается недостаточным для высокочастотных помех вследствие большой индуктивности протяжённых заземляющих проводников.

5. Реальные инциденты: как ЭМП уже нарушали работу энергообъектов.

Документированные случаи сбоев и повреждений оборудования демонстрируют многообразие сценариев реализации рисков и служат основой для совершенствования нормативных требований и технических решений. Однако следует отметить, что детальная информация об инцидентах на объектах критической инфраструктуры часто не публикуется по соображениям безопасности, что затрудняет формирование полной статистической картины

В 2022 году на территории Южного федерального округа России произошло более пятидесяти случаев выхода из строя терминалов РЗА вследствие воздействия грозовых импульсов, что составляет около 30 % от общего числа отказов оборудования за год. Типичным является случай на подстанции 110 кВ в Краснодарском крае, где близкий грозовой разряд индуцировал импульсные напряжения в кабелях системы телемеханики, что привело к одновременному повреждению четырёх микропроцессорных терминалов различных производителей. Солнечная активность в периоды геомагнитных бурь вызывает индуцирование геомагнитно-индуцированных токов (ГИТ) в протяжённых линиях электропередачи и заземляющих контурах подстанций. Сильная геомагнитная буря в марте 2024 года привела к возникновению квазипостоянных токов амплитудой до 50 А в нейтралях трансформаторов на подстанциях Северо-Западного региона России. Насыщение магнитопроводов трансформаторов вызвало искажение формы кривой тока намагничивания и ложные срабатывания дифференциальных защит, рассчитанных на синусоидальную форму тока. Два случая излишнего отключения трансформаторов были зафиксированы в период максимальной геомагнитной активности. Для предотвращения подобных ситуаций рекомендуется использование алгоритмов защиты, нечувствительных к постоянной составляющей тока, или установка устройств блокировки ГИТ в нейтралях трансформаторов.

Проведённое исследование позволяет сформулировать комплекс выводов относительно влияния электромагнитных помех на системы управления электроэнергетическими объектами как фактора риска для информационной безопасности. Перспективы дальнейших исследований связаны с разработкой интегрированных систем мониторинга электромагнитной обстановки с использованием искусственного интеллекта для предсказания опасных событий, созданием новых материалов и конструкций для эффективного экранирования.

УДК 621.395.87:004.056(045)

М. В. Кузнецова, В. А. Симонова,

обучающиеся 4 курса Института права,
социального управления и безопасности ФГБОУ ВО «УдГУ».
Научный руководитель: Т. Н. Стерхова, канд. техн. наук, доцент
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Акустическая охранная сигнализация на логических элементах

В современных условиях обеспечение безопасности объектов является одной из важнейших задач как для частных пользователей, так и для организаций. Значительная часть несанкционированных проникновений осуществляется через окна, стеклянные двери и витрины, поскольку именно стеклянные конструкции являются наиболее уязвимыми элементами охраняемого периметра. По некоторым оценкам, доля таких проникновений достигает 55 % от общего числа инцидентов, что почти вдвое превышает количество взломов дверей. В связи с этим широкое распространение получили акустические охранные сигнализации, предназначенные для обнаружения разрушения стекла по характерным звуковым признакам.

Актуальность использования акустических систем обусловлена тем, что подобные устройства позволяют контролировать одновременно несколько оконных конструкций в пределах одного помещения, что делает их более экономичными по сравнению с установкой отдельных контактных датчиков на каждую точку доступа. Дополнительным преимуществом является возможность применения методов цифровой обработки сигнала, существенно снижающих вероятность ложных срабатываний[138].

[138] Ложные срабатывания технических средств охранной сигнализации и методы борьбы с ними. URL: https://41.rosguard.gov.ru/uploads/2021/11/r0762018.pdf (дата обращения: 25.05.2026).

Акустическая охранная сигнализация представляет собой систему, реагирующую на звуковые колебания, возникающие при разрушении стеклянных поверхностей. Основным элементом таких систем является акустический извещатель, преобразующий звуковой сигнал в электрический. В состав акустического датчика обычно входят чувствительный элемент (микрофон), блок обработки сигналов, блок формирования тревожного извещения, источник питания и система индикации.

Современные охранные извещатели анализируют одновременно две составляющие сигнала разрушения стекла: низкочастотную и высокочастотную. Низкочастотная составляющая возникает в момент удара, в то время как высокочастотная соответствует звону разбитого стекла. Именно последовательность появления этих двух составляющих в определённом временном интервале позволяет устройству отличить реальное разрушение от случайного шума[139].

Акустические датчики нашли широкое применение в различных местах, включая финансовые учреждения, офисные пространства, торговые комплексы, жилые помещения и складские объекты. Каждый датчик способен охватывать территорию радиусом до 8–10 метров, что позволяет контролировать одновременно несколько оконных проемов.

В ходе проведенного исследования была создана упрощенная модель охранной сигнализации, основанная на логических элементах и выполнено её моделирование в программе Micro-Cap (рис. 1). В состав схемы входили логические элементы «НЕ-И», резисторы, конденсаторы, диоды, транзисторы, источник питания 12 В, переключатели и светодиодный индикатор. Основным элементом системы являлся геркон, выполняющий функцию датчика состояния двери. При закрытой двери контакты геркона находились в замкнутом состоянии, а при открытии – размыкались, что приводило к изменению логического сигнала на входе схемы.

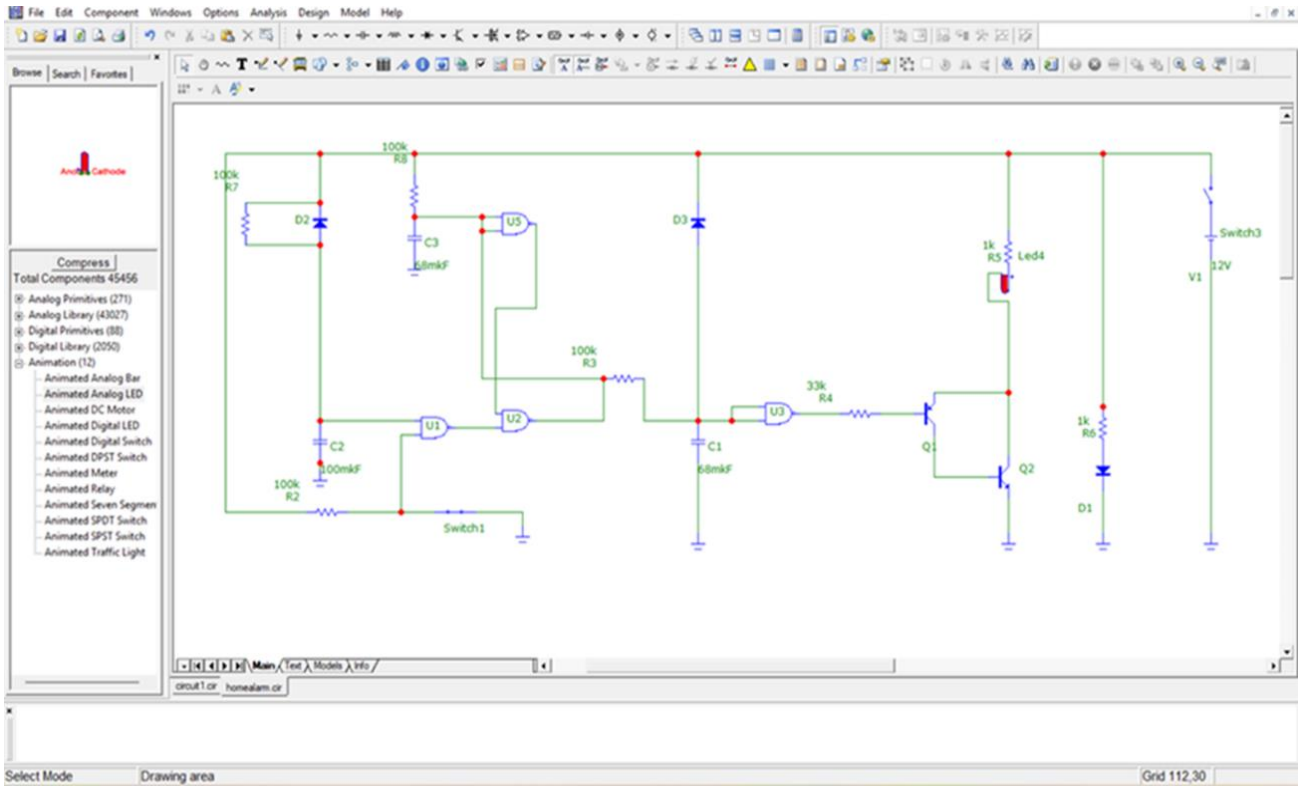


Рис. 1. Схема при замкнутом герконе

В качестве логического блока использовались элементы «НЕ-И». Особенностью данных элементов является формирование логического нуля только при наличии логической единицы на всех входах одновременно. Во всех остальных случаях на выходе формируется логическая единица. Работа схемы была организована следующим образом: при закрытой двери система находилась в дежурном режиме; при открытии двери изменялся сигнал с геркона; логические элементы переключались; запускалась RC-цепь задержки; сигнал поступал на усилительный каскад; включался индикатор тревоги.

[139] Системы охранной, пожарной и охранно-пожарной сигнализации. URL: https://djvu.online/file/nMd1pigzichei (дата обращения: 25.05.2026).

Для формирования временной задержки использовались RC-цепи, состоящие из резисторов и конденсаторов. Конденсаторы заряжались постепенно, благодаря чему тревожный сигнал формировался спустя небольшой промежуток времени. Это позволяло уменьшить вероятность ложных срабатываний при кратковременных помехах.

Усилительный каскад был реализован на транзисторах различной структуры – NPN и PNP. Использование двух транзисторов позволяло увеличить мощность выходного сигнала и обеспечить управление внешней нагрузкой. В качестве исполнительного элемента использовался светодиод, выполняющий функцию индикации тревоги[140].

После сборки схемы было проведено моделирование работы системы в двух режимах – нормальной работы и тревоги. При закрытой двери геркон находился в замкнутом состоянии. На вход логических элементов поступал сигнал, поддерживающий схему в дежурном режиме. Светодиод не формировал тревожное извещение. При открытии двери геркон размыкался, логическая схема изменяла своё состояние, после чего через RC-цепь формировалась задержка включения. Далее транзисторный каскад усиливал сигнал, и включался индикатор тревоги. Проведённое моделирование показало корректную работу схемы и подтвердило возможность использования логических элементов для построения простейших охранных систем (рис. 2).

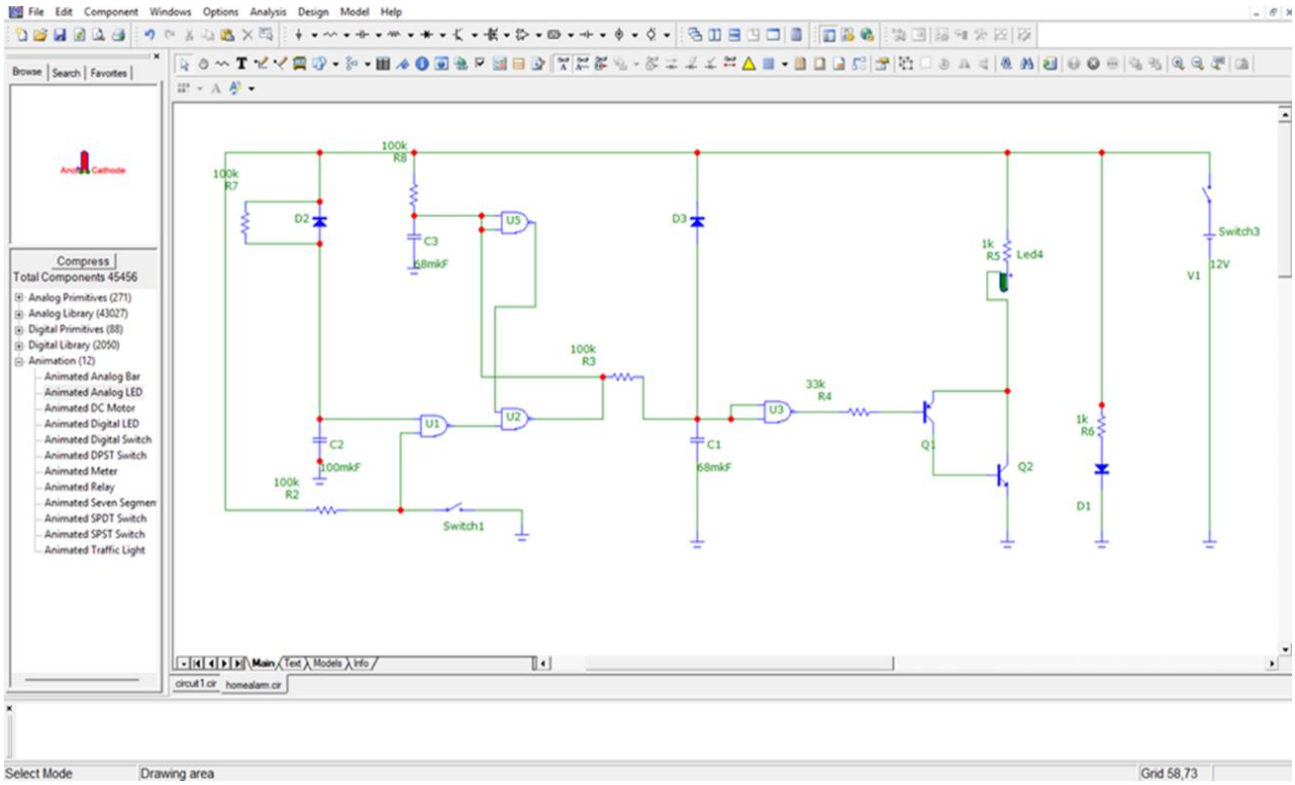


Рис. 2. Схема при разомкнутом герконе

Современные системы охранной сигнализации значительно отличаются от простых логических схем тем, что используют цифровую обработку звуковых сигналов. Одним из ключевых методов анализа является быстрое преобразование Фурье, позволяющее представить сигнал в частотной области и определить его спектральный состав.

Быстрое преобразование Фурье применяется для анализа спектра сигнала разрушения стекла. Характерной особенностью такого сигнала является наличие низкочастотного импульса удара и высокочастотного звона осколков. В современных акустических извещателях сигнал проходит несколько этапов обработки: микрофон принимает акустические колебания; аналоговый сигнал преобразуется в цифровой; выполняется быстрое преобразование Фурье; формируется спектр частот; спектр сравнивается с эталонным шаблоном разбития стекла; при совпадении формируется тревожный сигнал.

[140] Рябцев Н. А. Методические рекомендации. Выбор и применение охранных поверхностных звуковых извещателей для блокировки остекленных конструкций закрытых помещений / Н. А. Рябцев, Р. Ю. Воронков, А. Н. Федин [и др.]. М., 2024. URL: https://nicohrana.ru/wp-content/uploads/2024/12/r-044-2024-vybor-i-primenenie-ohrannyh-poverhnostnyh-zvukovyh-izveshhatelej.pdf (дата обращения: 25.05.2026).

Использование быстрого преобразования Фурье позволяет существенно повысить точность распознавания событий и снизить вероятность ложных срабатываний. Алгоритм БПФ основан на рекурсивном разбиении исходного сигнала на последовательности меньшей длины, благодаря чему количество вычислительных операций значительно сокращается по сравнению с прямым вычислением дискретного преобразования Фурье. Это позволяет выполнять спектральный анализ в режиме реального времени даже на микроконтроллерах с ограниченными вычислительными ресурсами[141].

Разработанная схема является базовой версией системы охраны, но с потенциалом для развития. Одним из перспективных путей усовершенствования является замена геркона на акустический датчик. Такая модификация позволит фиксировать разрушение стекла и контролировать большую площадь помещения. Другой перспективой будет являться применение микроконтроллеров. Это позволит добиться высокой степени адаптивности в настройке алгоритмов, осуществлять цифровую обработку поступающих данных, а также даст возможность последующего обновления программного обеспечения и внедрения продвинутых методик анализа звуковых сигналов.

Дополнитель, в системе возможна реализация беспроводной передачи данных через GSM или WI-FI, системы резервного питания, цифровой фильтрации помех, режима фиксации тревоги, а также интеграция в системы «умного дома». Подобные решения уже активно применяются в профессиональных охранных системах. В качестве примеров можно привести такие устройства, как акустические извещатели «Сонар»[142] и «Стекло-3»[143]. Они используют цифровую обработку сигнала и анализ спектра звука для обнаружения разрушения стекла.

Результаты проведенной работы демонстрируют, что даже простые логические схемы способны обеспечить выполнение основных задач для охранной защиты периметра. Применение методов цифровой обработки сигналов и быстрого преобразования Фурье существенно улучшит точность определения тревожных событий, тем самым минимизируя ложные срабатывания. Внедрение микроконтроллеров и интеллектуальных алгоритмов анализа звуковых характеристик позволит расширить функциональные возможности системы и повысит надежность охраны объектов.

УДК 004.89:004.92:378(045)

Д. В. Куренцов, Ф. В. Лимонов,
обучающиеся Института права,
социального управления и безопасности ФГБОУ ВО «УдГУ».
Научный руководитель: Т. Н. Стерхова, канд. техн. наук, доцент
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Проектирование интерактивной платформы для разработки лабораторного практикума и проведения лабораторных работ «SmartLab»

В рамках настоящего исследования авторами предлагается концептуальное решение по обеспечению информационной независимости образовательной среды. Описан опыт проектирования автономного комплекса SmartLab Assistant, в первую очередь ориентированного на подготовку специалистов для объектов критической инфраструктуры, а также подходящего для других технических специальностей, включающих в себя дисциплины электронного приборостроения. Раскрываются механизмы локализации данных и алгоритмизации учебных сценариев как инструменты повышения общей безопасности информационного взаимодействия.

Цифровизация современного высшего образования и стремительный переход к электронным форматам обучения требуют внедрения принципиально новых программных инструментов, способных обеспечить качественно высокий уровень интерактивности при сохранении простоты и надежности использования. Традиционные подходы к организации лабораторных практикумов, основанные

[141] Быстрое преобразование Фурье в цифровой обработке сигналов. URL: https://cyberleninka.ru/article/n/bystroe-preobrazovanie-furie-v-tsifrovoy-obrabotke-signalov?ysclid=mpff96hp5c788615244 (дата обращения: 25.05.2026).

[142] Извещатель охранный акустический ИО 329-17 «Сонар». URL: https://satro-paladin.com/catalog/product/38670/ (дата обращения: 25.05.2026).

[143] Стекло-3 (ИО 329-4), извещатель охранный поверхностный звуковой. URL: https://www.chipdip.ru/product/steklo-3-io-329-4-izveschatel-ohrannyy-poverhnostnyy-rielta-8038492288 (дата обращения: 25.05.2026).

на применении статических текстовых документов (форматов DOCX, PDF) или разрозненных веб-ресурсов, существенно ограничивают вовлеченность обучающихся, не обеспечивают сквозной контроль выполнения заданий и затрудняют оперативную адаптацию методических материалов под конкретные образовательные траектории. Более того, централизованные SaaS-платформы обладают критическими уязвимостями, связанными с необходимостью постоянного высокоскоростного интернет-соединения, рисками недоступности удаленных серверов и угрозами несанкционированной модификации данных извне.

В ответ на эти вызовы был разработан комплекс SmartLab Assistant – универсальная среда, объединяющая функции редактора, визуального симулятора и интеллектуального ассистента. Целью работы является описание архитектурных решений и функциональных возможностей данной системы[144].

В отличие от классических программ просмотра документов, где студент вынужден линейно прокручивать многостраничные файлы методических указаний, в SmartLab Assistant реализована концепция пошаговой дискретной подачи материала, получившая название «карусель действий».

Весь лабораторный процесс разделяется на последовательность атомарных слайдов (шагов). Каждый шаг жестко координирует действия пользователя, отображая только ту информацию, которая необходима на данном этапе (теория, текущая формула, интерактивное мини-задание). Переход к следующему шагу может быть заблокирован системой до тех пор, пока студент не выполнит текущие требования (например, не соберет правильную схему или не введет верный расчетный коэффициент), что реализует концепцию управляемого образовательного трека. Внутренний редактор графических элементов SmartLab интегрирует функции графического построения с атрибутивным наполнением объектов. Процесс соединения узлов в режиме «Провод» позволяет студентам не просто визуализировать топологию сети, но и настраивать качественные характеристики связей – цветность, градиент прозрачности и сечение. В контексте безопасности электросетей это служит для маркировки зон доверия и визуального аудита критических маршрутов передачи сигналов управления АСУ ТП[145].

Одной из главных проблем при внедрении интеллектуальных систем автоматизации является высокая трудоемкость оцифровки старых бумажных или текстовых методических указаний. Для решения этой задачи в SmartLab Assistant интегрирована специализированная консоль управления AI-Console. Внутри системы реализована функция process_ai_json, которая принимает на вход неструктурированный текст или полуструктурированные JSON-сценарии, сгенерированные внешними языковыми моделями, и автоматически производит синтаксический разбор контента.

Данный модуль налету распознает разделы лабораторной работы, вычленяет формулы LaTeX, генерирует необходимые шаги для «карусели действий», автоматически подтягивает нужные компоненты в панель инструментов и выстраивает готовую интерактивную лабораторную работу. Применение AI-парсера позволяет преподавателю сократить время на подготовку и программирование одного интерактивного занятия более чем на 60 %, превращая рутинный процесс верстки в быструю автоматизированную сборку.

В ходе апробации прототипа было проведено исследование конкурентных преимуществ SmartLab в сравнении с общепринятыми форматами организации самостоятельной работы.

Таблица 1

Сравнительный анализ функциональных и эксплуатационных характеристик образовательных сред

Критерий оценки	Традиционные SaaS / Редакторы (Word, PDF)	Автономная среда SmartLab
Структура контента	Линейный статический текст, низкая вовлеченность, ручной скроллинг	Интерактивная пошаговая карусель действий с фиксацией этапов
Математический аппарат	Статичные растровые картинки формул или тяжелые внешние OLE-объекты	Динамический Live Preview LaTeX на базе встроенного MathJax[146]
Моделирование схем	Использование стороннего ПО, экспорт внешних скриншотов	Встроенный интерактивный редактор связей и компонентов (Drag-and-Drop)
Доступность и безопасность	Зависимость от интернет-каналов, риск потери данных на сервере	Полная автономность (offline-first), локальный контроль формата .slabs

[144] ГОСТ Р 7.0.5-2008. Библиографическая ссылка. Общие требования и правила составления. М. : Стандартинформ, 2008.
[145] Документация фреймворка PyQt6. URL: https://www.riverbankcomputing.com/ (дата обращения: 22.04.2026).
[146] Описание библиотеки MathJax. URL: https://www.mathjax.org/ (дата обращения: 22.04.2026).

Разработанный программный подход демонстрирует высокую научно-практическую значимость в контексте построения изолированных, доверенных образовательных сред, полностью независимых от импортных инфраструктурных элементов и провайдеров облачных платформ. Архитектурный каркас SmartLab Assistant спроектирован с учетом легкого масштабирования и расширения функционала.

Дальнейшие векторы развития проекта лежат в области создания кроссплатформенной мобильной версии приложения на базе фреймворков, компилируемых из Python, что позволит реализовать современную концепцию непрерывного обучения (anytime, anywhere). Также научно-инженерный интерес представляет разработка и интеграция программного модуля для многопользовательской коллективной работы. Это позволит студентам объединяться в локальные группы для совместного проектирования сложных комплексных схем и проведения комплексных инженерных исследований в режиме реального времени. Кроме того, ведется работа по расширению базовой библиотеки компонентов универсальными элементами для моделирования алгоритмических и цифровых систем общего назначения.

Результаты проектирования и практической реализации программного комплекса SmartLab Assistant позволяют сделать вывод о высокой эффективности децентрализованных автономных программных решений в рамках современного высшего образования. Создание изолированной локальной среды, объединяющей в себе теоретические интерактивные блоки, расчетно-формульные модули и полноценный схемотехнический редактор, минимизирует количество инфраструктурных точек отказа и устраняет внешние цифровые зависимости.

Разработанная платформа не только существенно упрощает для преподавателей процессы генерации, верификации и оцифровки лабораторных практикумов с применением механизмов интеллектуального парсинга, но и кардинально повышает качество освоения материала студентами технических специальностей, формируя у них устойчивые навыки работы с современным прикладным программным обеспечением.

УДК 342.9:004(045)

М. С. Ложкина,
обучающаяся 3 курса Института права,
социального управления и безопасности ФГБОУ ВО «УдГУ».
Научный руководитель: Е. А. Яковлева, ассистент
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Верификация как метод правового регулирования в государственном управлении

Цифровизация государственных функций и рост объёмов информационного обмена дали управленческие преимущества, но одновременно создали новые угрозы. Рост числа кибератак на государственные сервисы, платформы и приложения вынуждает пересматривать сложившиеся подходы к правовому регулированию. Правовое регулирование направлено на соблюдение законности и правопорядка в обществе и предусматривает ответственность за совершённое нарушение. Вместе с тем правовые процедуры, нацелены на подтверждение достоверности данных субъектов и их идентификацию, при которых обеспечивается конфиденциальность информации для решения приоритетных задач государственного управления.

Запреты и санкции сами по себе не обеспечивают достоверности информации, необходимой для принятия управленческих решений. Дозволения, обязывания и запреты перестают работать там, где информационная среда меняется быстрее законодательного реагирования. Таким образом, техническое регулирование становится приоритетным направлением, обеспечивающим некую защищенность субъектов и объектов информационной среды. В то время как правовое регулирование оказывает непосредственное воздействия на правоотношения в информационной сфере.

Также, в теории права метод правового регулирования определяется как сочетание способов воздействия права на общественные отношения. Характер такого сочетания задаёт отраслевой режим регулирования Государственное управление реализуется через деятельность органов законодательной, исполнительной и судебной власти[147]. Правовые предписания, устанавливающие необходимость

[147] Бахрах Д. Н., Россинский Б. В., Старилов Ю. Н. Административное право : учебник для вузов. 3-е изд., пересмотр. и доп. М. : Норма, 2008. С. 28.

подтверждения соответствия данных и идентификации субъектов, образуют самостоятельный метод правового регулирования в государственном управлении.

Тем не менее терминологическую основу верификации задаёт ГОСТ Р ИСО 9000-2015. В этом стандарте верификация определена как подтверждение факта выполнения установленных требований, которое опирается на объективные свидетельства. В сфере государственного управления данное понятие получает дополнительное содержание. Верификация приобретает характер самостоятельного административно-правового метода, не сводимого к технической проверке. Метод сводится к сопоставлению сведений, полученных от пользователя, с нормативно закреплёнными критериями достоверности, полноты и надежности информации. Результатом такого сопоставления выступает прямое упорядочение отношений в информационной сфере. Оно охватывает и допуск к государственным услугам, и фиксацию юридически значимых фактов.

Содержание метода раскрывается в отраслевых и функциональных нормативных актах. Приказ Росреестра от 23.11.2010 № П/618 «Об организации работ по повышению качества данных единого государственного реестра прав и государственного кадастра недвижимости»[148] впервые закрепил верификацию как процедуру государственного управления. Документ предписывал проведение верификации данных для повышения их целостности, взаимоувязанности и исключения утраты сведений.

Установленные данным правовым актом признаки верификации применимы за пределами кадастрового учёта. К ним относятся: проверка данных на соответствие нормативным требованиям и подтверждение их совпадения с информацией из правоустанавливающих документов.

Законодательство содержит правовые требования к организации и порядку верификации, формирующие искомый метод. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[149] закрепляет принцип достоверности информации. Данный принцип предполагает обязанность государства проверять соответствие информации реальному положению дел. Верификация служит императивным механизмом его обеспечения.

Вместе с тем ГОСТ Р 72297-2025 «Государственное управление. Качество данных официального статистического учета»[150] устанавливает требования к качеству данных официального статистического учёта. Он призван поддерживать доверие к официальной статистике у государственных органов, делового сообщества, учёных и граждан. И как отмечает Е. А. Яковлева: «Для этого необходимо создать специальный правовой регуляторный механизм для информационных правоотношений, отвечающий за приём, обработку и передачу информации по защищенным каналам связи, где стратегически главным обстоятельством, требующим регуляторного влияния будет укрепление доверия к информационному ресурсу, к информационному процессу и организации, участвующей в информационном взаимодействии»[151]. В числе критериев оценки качества данных и повышения уровня доверия верификация является специфическим методом регулирования, распространение которого возможно в информационной сфере.

Формируемый метод охватывает и сертификацию средств защиты информации. Согласно актам Правительства РФ[152] и ФСТЭК России[153], средства, предназначенные для защиты конфиденциальной информации, подлежат обязательной сертификации. Эта процедура сводится к верификации продукта на соответствие требованиям по безопасности информации. Государственная информационная система не может эксплуатироваться без оформленных прав на её компоненты, включая средства защиты.

Формируемый метод включает подтверждение легитимности программного обеспечения. Постановлением Правительства РФ от 28.11.2025 № 1931 «Об утверждении Правил формирования и ведения перечня доверенных российских программ для электронных вычислительных машин и баз данных»[154] утверждены правила ведения перечня доверенных российских программ для ЭВМ и баз

---

[148] Об организации работ по повышению качества данных единого государственного реестра прав и государственного кадастра недвижимости : приказ Росреестра от 23.11.2010 № П/618 // СПС «Гарант» (дата обращения: 17.04.2026).

[149] Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 № 149-ФЗ // СЗ РФ. 2006. № 31 (ч. 1). Ст. 3448.

[150] Государственное управление. Качество данных официального статистического учета: ГОСТ Р 72297-2025. М. : Рос. ин-т стандартизации, 2025.

[151] Яковлева Е. А. Правовые проблемы цифровой доверенной среды // Вестник Удмуртского университета. Серия «Экономика и право». 2023. Т. 33, № 1. С. 181–186.

[152] О сертификации средств защиты информации : постановление Правительства РФ от 26.06.1995 № 608 // СЗ РФ. 1995. № 27. Ст. 2579.

[153] Об утверждении Положения о системе сертификации средств защиты информации : приказ ФСТЭК России от 03.04.2018 № 55 (зарегистрирован в Минюсте России) // СПС «КонсультантПлюс» (дата обращения: 18.04.2026).

[154] Об утверждении Правил формирования и ведения перечня доверенных российских программ для электронных вычислительных машин и баз данных : постановление Правительства РФ от 28.11.2025 № 1931. URL: https://normativ.kontur.ru/document?moduleId=1&documentId=503077 (дата обращения: 18.04.2026).

данных. Включение программного обеспечения в такой перечень подтверждает его соответствие критериям доверенности, обязательным для государственных информационных систем.

Верификация применяется за рамками технического и информационного регулирования, что подтверждается международными актами. Так, например, решение Совета Евразийской экономической комиссии[155] определяет верификацию как установление подлинности сертификата о происхождении товара и достоверности содержащихся в нём сведений. Вместе с тем он закрепляет понятие верифицирующего органа. В международном праве правовое регулирование верификации включает субъектный состав, процедуру и правовые последствия. В данном контексте верификация устанавливает подлинность юридических фактов.

Перечисленные нормативные правовые акты образуют систему, основанную на общих принципах: объективность и независимость проверки, документированность процесса, строгое соответствие законодательству. Эти принципы формируют метод, основанный на процедуре подтверждения юридически значимого качества объекта (информации, продукта или документа).

Отсутствие легального определения верификации как метода государственного управления и общеправового понятия качества информации препятствует оформлению юридической силы данного метода. Законодатель фактически применяет верификацию в ряде сфер, однако не закрепляет её нормативного определения. В сертификации средств защиты информации верификация сводится к государственной экспертизе, тогда как в кадастровом учёте она ограничивается сопоставлением данных электронной базы с бумажным оригиналом. Подобные расхождения при отсутствии единой законодательной основы не позволяют сформировать единообразную правоприменительную практику.

Отсутствие правового контроля за верификацией в информационной среде влечёт риск злоупотреблений и снижает доверие к государственным информационным ресурсам. Правовое регулирование в этой сфере не успевает за технологическим развитием и не устанавливает необходимых нормативных ограничений.

Нормы верификации образуют метод правового регулирования. Однако он не закреплен в законе, поскольку определение верификации как административной процедуры отсутствует.

Законодательство не закрепляет за верификацией статуса юридически значимого действия, оставляя её лишь инструментом. Между тем от достоверности сведений, которыми располагают государственные органы, зависит обеспеченность прав и свобод граждан.

Органы должны проверять важные для государства сведения. Подобное решение укрепит информационную безопасность и повысит эффективность управления, опирающегося на достоверные данные.

УДК 004.056:378(045)

И. Р. Муллаяров,
обучающийся 3 курса экономико-математического факультета
Нефтекамского филиала ФГБОУ ВО «Уфимский университет науки и технологий».
Научный руководитель: А. Р. Аюпова, канд. физ.-мат. наук, доцент
Нефтекамского филиала ФГБОУ ВО «Уфимский университет науки и технологий»,
г. Нефтекамск

Обеспечение безопасности персональных данных в вузе: аналитический обзор и разработка системы

На сегодняшний день защита информации является одной из наиболее актуальных и значимых проблем. Образовательные организации, как и любая другая организация, имеет дело с большим объемом конфиденциальных данных, которые становятся объектом интереса для злоумышленников.

Цифровая трансформация показывает огромный потенциал для преобразования различных отраслей экономики, и образование не является исключением.

Особое место во всем информационном потоке занимают персональные данные (ПДн) – сведения, относящиеся к прямо или косвенно определенному или определяемому физическому лицу.

[155] Об утверждении Правил определения происхождения товаров из развивающихся и наименее развитых стран: Решение Совета Евразийской экономической комиссии от 14.06.2018 № 60 // Официальный сайт Евразийского экономического союза. URL: https://www.alta.ru/tamdoc/18sr0060/ (дата обращения: 18.04.2026).

Инциденты, связанные с компрометацией персональных данных, наносят организациям колоссальный ущерб. Согласно отчетам аналитических центров (например, InfoWatch), в 2024–2025 гг. Россия столкнулась с беспрецедентным ростом числа утечек, затронувших миллионы граждан. Увеличивается как число, так и сложность кибератак, направленных на государственные и коммерческие объекты. Ущерб исчисляется не только прямыми финансовыми потерями в виде штрафов со стороны регуляторов (Роскомнадзор, ФСТЭК), но и невосполнимым репутационным вредом.

Несмотря на наличие правовой базы и широкого спектра технических средств защиты, проблема обеспечения реальной безопасности ПДн остается острой. Это связано как с постоянным развитием киберугроз (атаки программ-вымогателей, изощренный фишинг, кибершпионаж), так и со сложностью внедрения комплексной системы защиты, которая должна охватывать правовые, организационные и технические аспекты. Разработка специализированного программного обеспечения, изначально спроектированного с учетом требований законодательства (Privacy by Design), является одним из эффективных путей решения этой проблемы.

Целью данного исследования является анализ теоретических и практических аспектов защиты персональных данных и разработка концепции программного обеспечения для их безопасного сбора и обработки в соответствии с требованиями российского законодательства в образовательном учреждении.

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» определяет персональные данные как «любую информацию, относящуюся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)». К таким данным можно отнести: ФИО, дату и место рождения, адрес, семейное положение, сведения об образовании, доходы, номер телефона, адрес электронной почты, а также технические идентификаторы, такие как IP-адрес или cookie, если они позволяют идентифицировать субъекта.

Для современных организаций значение персональных данных двояко. С одной стороны, ПДн являются ценнейшим активом. На их основе строятся маркетинговые стратегии, управляется взаимодействие с клиентами (CRM-системы), ведется кадровый учет (1С:ЗУП). Качественные и полные данные о клиентах позволяют компании предлагать востребованные услуги и повышать свою конкурентоспособность.

С другой стороны, владение персональными данными накладывает на организацию (оператора ПДн) серьезную ответственность. Необходимость защиты ПДн диктуется тремя основными факторами: законодательные требования, репутационные риски, прямые финансовые потери.

Таким образом, эффективная система защиты ПДн – это не просто выполнение формальных требований, а критически важный элемент управления рисками и обеспечения устойчивости бизнеса, основанный на принципах конфиденциальности, целостности и доступности информации (триада CIA).

Угрозы безопасности ПДн – это совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения их конфиденциальности, целостности или доступности. Угрозы принято делить на намеренные и случайные, а также на внутренние и внешние. Согласно статистике (например, от Positive Technologies), в последние годы доминируют атаки со стороны внешних злоумышленников, однако внутренние угрозы (инсайдеры) часто приводят к наиболее крупным утечкам.

К внешним угрозам, представляющим наибольшую опасность для информационных систем, относятся целенаправленные хакерские атаки, вредоносное программное обеспечение, приёмы социальной инженерии и перехват данных в каналах связи.

Все же одной из наиболее значимых категорий рисков для информационной безопасности являются внутренние угрозы, исходящие от сотрудников организации или лиц, имеющих законный доступ к информационным системам. К внутренним угрозам подразумевают:

– умышленные действия сотрудников: Кража или «слив» баз данных конкурентам, использование ПДн в личных мошеннических целях. По данным InfoWatch, на долю инсайдеров приходится значительная часть всех утечек[156];

– неумышленные действия (халатность): наиболее частая причина инцидентов. Это случайное удаление данных, отправка письма с ПДн не тому адресату, использование простых паролей («123456», «qwerty»), утеря незашифрованного ноутбука или флеш-накопителя. Низкая киберграмотность персонала является существенным фактором риска.

Ключевым документом, определяющим технические требования к защите ПДн, является приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных

[156] Аналитический отчет «Утечки информации ограниченного доступа в России 2024–2025». URL: https://www.infowatch.ru/sites/default/files/analytics/files/rossiya-utechki-informatsii-ogranichennogo-dostupa-2024-2025.pdf (дата обращения: 12.02.2026).

и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Процесс выбора мер защиты включает:

– определение УЗ. Используется постановление № 1119 на основе типа угроз, категории ПДн и объема данных;

– определение базового набора мер. Для выбранного УЗ из приказа № 21 выбирается соответствующий базовый набор мер;

– адаптация базового набора мер. Уточнение, дополнение или исключение мер на основе модели угроз безопасности ПДн, специфичной для данной ИСПДн[157];

– выбор СЗИ. Подбор сертифицированных ФСТЭК (и ФСБ для криптографии) средств защиты информации для реализации выбранных мер.

В большинстве организаций ПДн обрабатываются не в какой-то одной, а в целом комплексе информационных систем, которые часто тесно интегрированы между собой:

– системы кадрового учета и расчета заработной платы (1С:ЗУП, БОСС-Кадровик): Одни из основных ИСПДн в любой компании. Хранят полный набор данных о сотрудниках, включая паспортные данные, ИНН, СНИЛС, сведения о семье, образовании, а иногда и специальные категории (данные о здоровье в больничных листах);

– системы управления взаимоотношениями с клиентами (CRM): (Bitrix24, amoCRM, RetailCRM). Хранят ПДн клиентов: ФИО, телефоны, e-mail, историю покупок. Уровень защищенности здесь часто ниже, чем в кадровых системах, что делает их привлекательной целью для атак;

– системы контроля и управления доступом (СКУД): (Perco, Sigur). Собирают биометрические данные (отпечатки пальцев, снимки лиц) и ведут учет времени прихода/ухода сотрудников;

– веб-сайты и интернет-магазины: (на CMS 1С-Битрикс, Tilda, самописные). Собирают ПДн через формы регистрации, обратной связи, оформления заказов;

– медицинские информационные системы (МИС): (Инфоклиника, MedWork). В клиниках и больницах обрабатывают специальные категории ПДн.

Практической частью работы явилось создание автоматизированной информационной системы (АИС) «Журнал куратора», предназначенной для безопасного сбора, хранения и обработки персональных данных студентов в образовательном учреждении, а именно в вузе, где развит кураторский институт. Основные задачи, решаемые программным комплексом:

– автоматизация учета студентов и учебных групп;

– разграничение прав доступа к информации на основе ролевой модели (Администратор, Куратор, Студент);

– обеспечение конфиденциальности критических персональных данных (паспортные данные, ИНН, СНИЛС и др.) посредством шифрования;

– ведение журнала событий безопасности для контроля действий пользователей.

В качестве архитектурного решения выбрано настольное приложение. Выбор обусловлен необходимостью хранения данных на локальном сервере без передачи их на сторонние облачные серверы, что повышает уровень защищенности.

Технологический стек разработки:

– написан на языке программирования – python 3.12. Выбор обоснован наличием мощных библиотек для криптографии и кроссплатформенностью;

– фреймворк PySide6 обеспечивает современный и отзывчивый интерфейс;

– используется встраиваемая база данных, файл которой хранится локально (app.db). Это упрощает развертывание и резервное копирование;

– библиотека cryptography для шифрования данных и стандартный модуль hashlib для хэширования паролей.

Структура приложения построена по модульному принципу:

– main.py – точка входа в приложение;

– database.py – слой работы с данными (шифрование, подключение к БД);

– mainwindow.py – главное окно приложения и логика переключения вкладок;

– widgets.py – реализация интерфейсов для разных ролей (администратор, куратор, студент);

– dialogs.py – диалоговые окна (вход в систему, настройки, создание пользователей.

[157] Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных : постановление Правительства РФ от 01.11.2012 № 1119 // СПС «КонсультантПлюс» (дата обращения: 12.02.2026).

Таким образом, был проведен комплексный анализ проблемы и разработана архитектура программного решения, соответствующего актуальным требованиям законодательства РФ в области защиты персональных данных. Дальнейшим развитием работы может стать полная реализация данного приложения и его развертывание в тестовой среде для проведения полного цикла испытаний на соответствие мерам защиты.

УДК 621.3.013:004.94(045)

А. М. Нигматуллин, В. А. Фёдоров,
обучающиеся 2 курса Института права,
социального управления и безопасности ФГБОУ ВО «УдГУ».
Научный руководитель: Т. Н. Стерхова, канд. техн. наук, доцент
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Исследование переходных процессов в RLC-цепях

Работа посвящена анализу переходных явлений в последовательном RLC-контуре под действием импульсного сигнала. Рассмотрены колебательный, критический и апериодический режимы функционирования. Посредством компьютерного моделирования определено значение критического сопротивления, получены временные диаграммы тока и напряжения. Проведено сопоставление расчётных и экспериментальных данных.

Ключевые слова: RLC-контур, переходной процесс, колебательный режим, критическое сопротивление, апериодический режим, имитационное моделирование.

Под переходными процессами понимают процессы перехода от одного установившегося режима работы электрической цепи к другому, чем-либо отличающемуся от предыдущего, например: величиной амплитуды, фазы, частоты или значениями параметров схемы[158].

Актуальность темы обусловлена тем, что подавляющее большинство современных электронных систем функционирует в условиях непрерывного изменения входных сигналов. Пуск оборудования, передача информационных импульсов, коммутация нагрузок – все эти операции сопровождаются переходными режимами, определяющими такие характеристики устройств, как помехоустойчивость, скорость отклика и эксплуатационная надёжность

Применение методов имитационного моделирования открывает возможность не только верифицировать аналитические выкладки, но и визуализировать динамику электромагнитных процессов при варьировании параметров компонентов схемы.

Цель этой работы состоит в выявлении закономерностей влияния величины активного сопротивления на характер протекания переходного процесса в последовательном RLC-контуре при подаче импульсного напряжения, а также в том, чтобы найти критическое сопротивление и экспериментальном наблюдении трёх режимов: колебательного, критического и апериодического.

Для реализации поставленной цели потребовалось: изучить теоретические основы анализа переходных процессов в цепях второго порядка; смоделировать виртуальную модель последовательного RLC-контура; вычислить величину критического сопротивления; выполнить серию вычислительных экспериментов для различных значений R; проанализировать осциллограммы напряжения на ёмкостном элементе и тока ветви; сопоставить полученные данные с теоретическими зависимостями и сформулировать выводы о роли активного сопротивления в формировании динамических характеристик контура.

Последовательный RLC-контур образован тремя элементами – резистором, катушкой индуктивности и конденсатором, соединёнными последовательно

Математическое описание процессов, протекающих в такой цепи, базируется на законах Кирхгофа и компонентных уравнениях элементов. Для последовательного соединения второй закон Кирхгофа утверждает, что сумма падений напряжений на всех элементах равна напряжению источника. Напряжение на резисторе подчиняется закону Ома, напряжение на индуктивности пропорцио-

[158] Таранов А. В. 3 Лекция ТОЭ-2 // Теоретические основы электротехники 2. URL: https://edu.kstu.kz/pluginfile.php/178663/mod_resource/content/1.pdf (дата обращения: 14.05.2026).

нально скорости изменения тока, а напряжение на конденсаторе связано с накопленным зарядом. Комбинируя эти соотношения, получаем линейное дифференциальное уравнение второго порядка:

$L \cdot d^2i/dt^2 + R \cdot di/dt + i/C = 0$

Данное уравнение является однородным, его решение состоит из свободной составляющей, определяемой начальными условиями и параметрами схемы. Характеристическое уравнение, соответствующее данному дифференциальному уравнению, записывается как $L \cdot p^2 + R \cdot p + 1/C = 0$. Его корни могут быть либо вещественными различными, либо вещественными равными, либо комплексно-сопряжёнными – в зависимости от знака дискриминанта.

Вид решения данного уравнения зависит от дискриминанта характеристического полинома, который, в свою очередь, определяется соотношением между параметрами схемы. Принято выделять три качественно различных сценария: колебательный ($R<R_{кр}$), при котором в цепи наблюдаются затухающие синусоидальные колебания; критический ($R=R_{кр}$), обеспечивающий наиболее быстрый выход на установившийся режим без перерегулирования; апериодический ($R>R_{кр}$), когда процесс носит монотонный затухающий характер[159].

Граница между режимами определяется критическим сопротивлением, вычисляемым по формуле:

$R_{кр}=2\sqrt{(L/C)}$

Собственная частота незатухающих колебаний определяется известным соотношением Томсона: $T=2\pi\sqrt{(LC)}$. Данная формула справедлива для идеального контура без потерь и даёт верхнюю оценку частоты колебаний реального контура. В реальных условиях наличие активного сопротивления приводит к уменьшению частоты свободных колебаний по сравнению с резонансной частотой, причём тем сильнее, чем больше величина R.

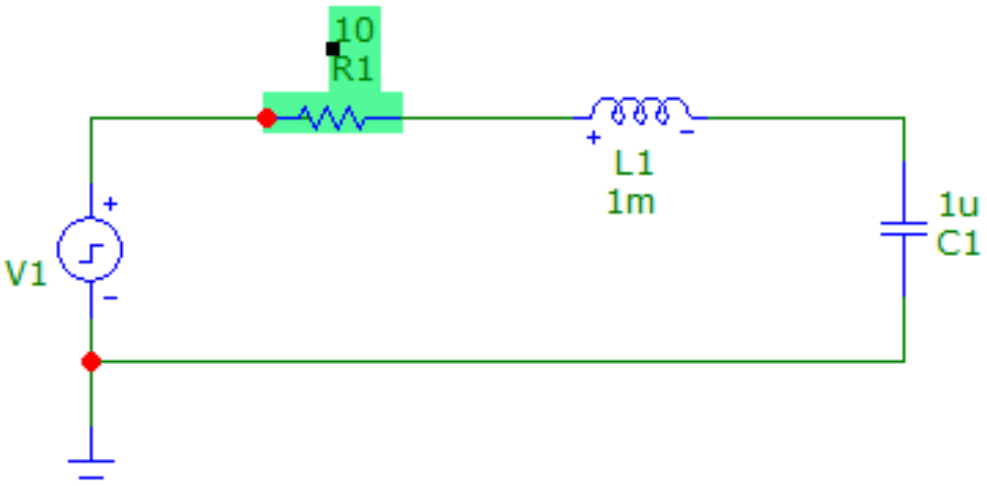


Рис. 1. Схема последовательного RLC-контура

В ходе работы и составления схемы, показанной на рис. 1, использовались следующие номиналы компонентов: индуктивность L=1 мГн, ёмкость C=1 мкФ. Величина резистора принимала три значения, соответствующие различным режимам:

– R_1=10 Ом (колебательный режим);
– R_2≈63,2 Ом (критический режим);
– R_3=500 Ом (апериодический режим).

С использованием пакета схемотехнического моделирования была построена модель последовательного RLC-контура, включающая источник прямоугольных импульсов, линейный резистор, катушку и конденсатор. Для каждого из трёх значений сопротивления выполнялся расчёт переходной характеристики с фиксацией осциллограмм тока в цепи и напряжения на обкладках конденсатора.

Колебательный режим (R_1 = 10 Ом).

На осциллограмме, показанной на рис. 2 зафиксированы затухающие гармонические колебания, период которых хорошо согласуется с теоретической оценкой (порядка 0,2 мс). Амплитуда колебаний экспоненциально убывает вследствие диссипации энергии в активном сопротивлении.

Критический режим ($R_2 \approx 63{,}2$ Ом).

[159] Переходные процессы в последовательной RLC-цепи // StudFile. URL: https://studfile.net/preview/9165610/page:7/ (дата обращения: 14.05.2026).

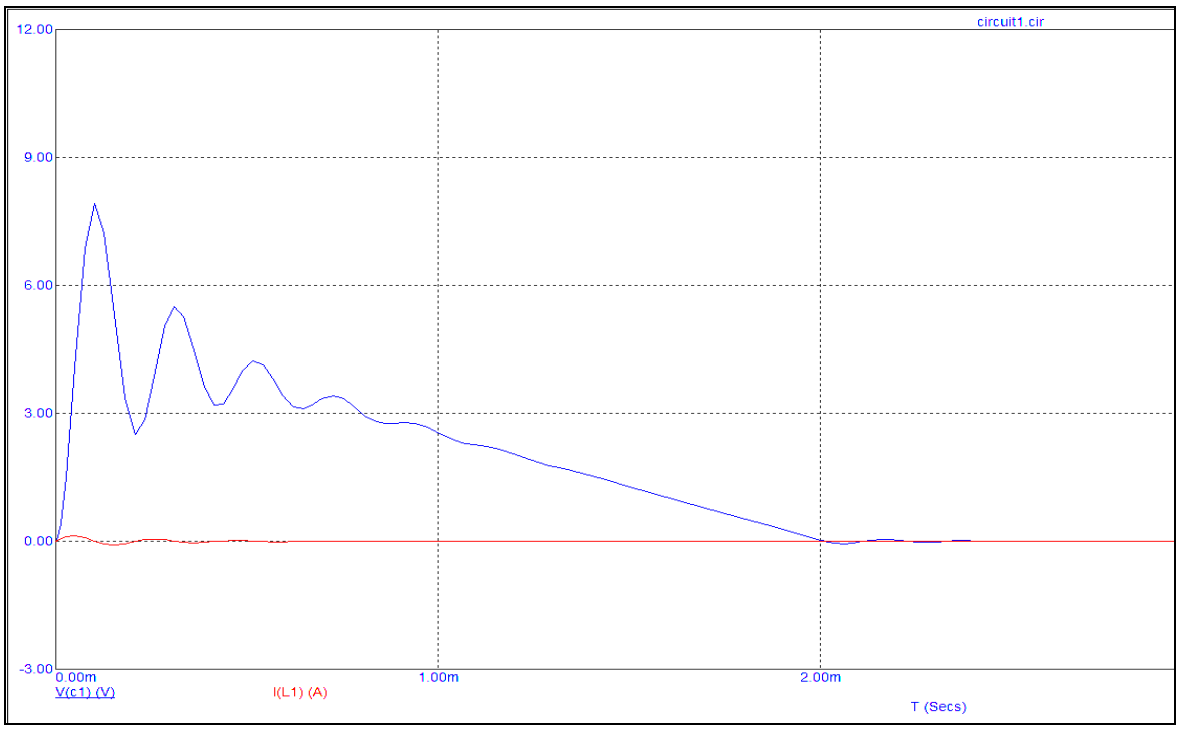


Рис. 2. Осциллограмма переходного процесса в колебательном режиме

При данном сопротивлении (см. рис. 3) переходная характеристика не содержит колебательной составляющей. Выход на установившееся значение происходит за минимально возможное время без превышения (перерегулирования), что характерно для граничного случая между колебательным и апериодическим режимами.

Апериодический режим ($R_з$ = 500 Ом).

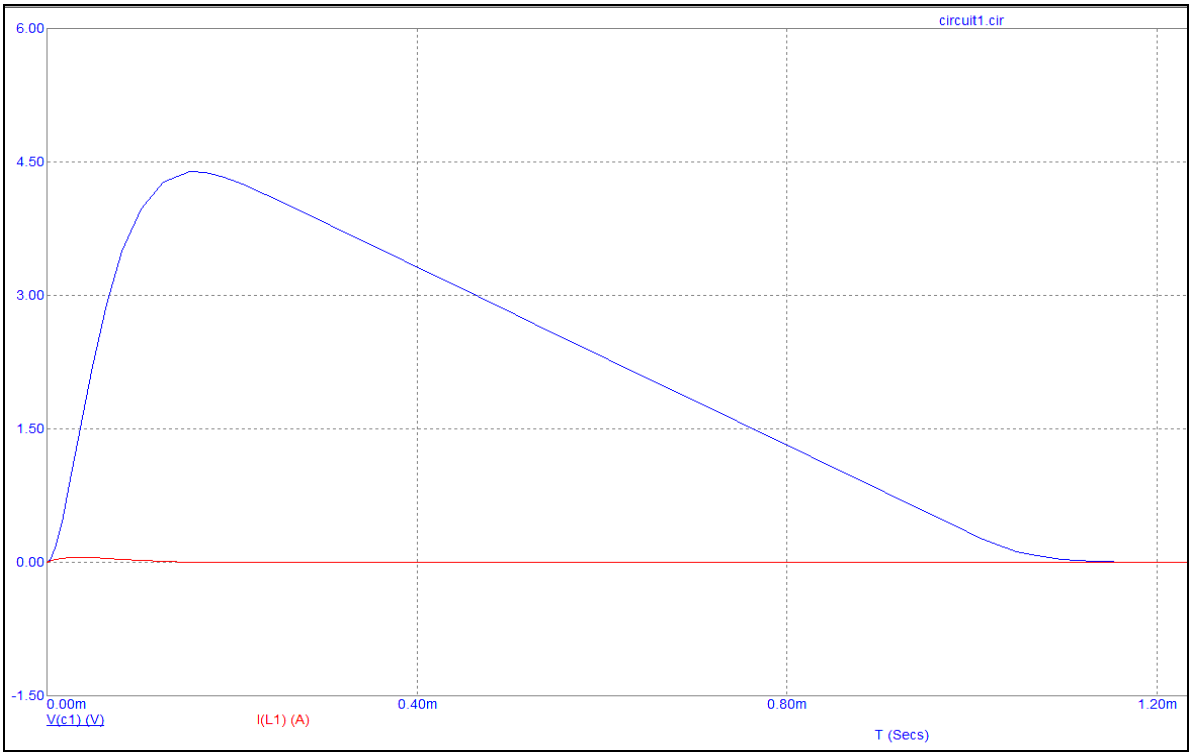


Рис. 3. Осциллограмма переходного процесса в критическом режиме

При большом активном сопротивлении как на рис. 4 колебательные явления отсутствуют, однако длительность переходного процесса существенно возрастает по сравнению с критическим случаем, что объясняется преобладанием диссипативных процессов над обменом энергии между реактивными элементами.

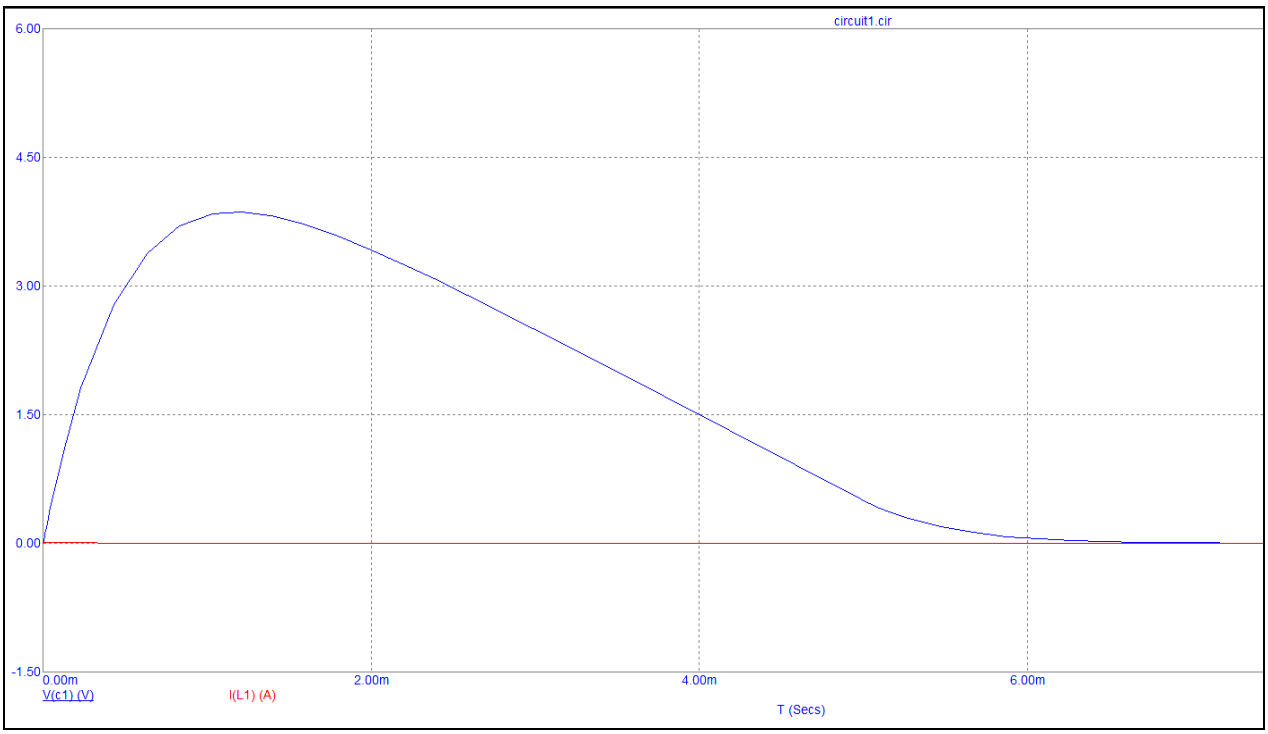


Рис. 4. Осциллограмма переходного процесса в Апериодическом режиме

Выполненные исследования подтверждают, что варьирование активного сопротивления является эффективным способом управления динамическими свойствами последовательного RLC-контура. При малых значениях R в цепи возникают затухающие колебания, при достижении критической величины процесс становится апериодическим с минимальным временем затухания, а дальнейшее увеличение сопротивления приводит к монотонному, но более длительному переходу. Полученные результаты могут быть использованы при проектировании фильтрующих цепей, импульсных преобразователей и систем автоматического регулирования, где требуется обеспечение заданного характера переходной характеристики.

УДК 342.7:004(045)

Д. А. Писканов,
обучающийся 3 курса Института права,
социального управления и безопасности ФГБОУ ВО «УдГУ».
Научный руководитель: Т. Н. Стерхова, канд. техн. наук, доцент
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Защита персональных данных пользователей в цифровой среде. Анализ угроз и методы минимизации рисков

Цифровая среда пронизывает все сферы жизни современного человека: от социальных сетей до получения государственных услуг. Персональные данные (ПДн) стали ценным товаром на чёрном рынке, а количество утечек данных растёт экспоненциально. При этом многие пользователи добровольно предоставляют доступ к своим данным, не оценивая связанные с этим риски. Ключевая проблема заключается в том, что контроль над персональными данными нередко переходит к корпорациям и злоумышленникам.

Целью работы является выявление основных каналов утечки персональных данных пользователей и разработка практических мер защиты. В задачи исследования входит: классификация типов собираемых данных, анализ реальных случаев утечек, оценка рисков от перехвата и анализа данных, разработка правил «цифровой гигиены», а также сравнение методов защиты (VPN, пароли, двухфакторная аутентификация).

Персональные данные традиционно подразделяются на несколько категорий:

– общедоступные (ФИО, должность);
– биометрические (отпечатки пальцев, лицо, голос);
– иные данные (телефон, email, местоположение, история покупок, IP-адрес).

Особенность современных цифровых систем заключается в том, что даже совокупность «безопасных» на первый взгляд данных позволяет однозначно идентифицировать человека.

К основным угрозам в цифровой среде относятся:

– фишинг – кража логинов и паролей через поддельные сайты;
– сбор данных без согласия – трекеры, куки, приложения, запрашивающие избыточные разрешения;
– утечки из баз данных – взлом серверов компаний (банков, магазинов, государственных органов);

Анализ показывает, что данные становятся легкодоступными для злоумышленников по нескольким причинам. Пользователи часто повторяют пароли или используют простые комбинации. Многие приложения запрашивают доступ к контактам, микрофону, геолокации «для удобства», хотя такой доступ не является необходимым для их основной функциональности. Законодательство в области защиты персональных данных зачастую отстаёт от темпов развития технологий[160].

В ходе исследования был смоделирован типовой сценарий атаки:

1. Пользователь устанавливает бесплатное приложение «Фонарик».
2. Приложение запрашивает доступ к контактам, камере и GPS.
3. Пользователь, не читая предупреждений, предоставляет разрешения.
4. Приложение в фоновом режиме собирает данные и отправляет их на сервер злоумышленника.
5. Собранные данные продаются или используются для целевого фишинга.

Для анализа подобных угроз применяются инструменты анализа сетевого трафика (например Wireshark) и контроля разрешений мобильных операционных систем (Android/iOS).

Цифровые сервисы используют несколько основных механизмов сбора информации:

– cookies и пиксели – для отслеживания поведения пользователей на сайтах;
– API трекеров (Google, Meta) – для объединения данных между различными сайтами;
– неявные разрешения – доступ к списку установленных приложений, аккаунту Google;
– анализ метаданных – фотографии часто содержат дату, место съёмки, модель устройства.

В совокупности эти механизмы позволяют создать детальный цифровой профиль человека, который может использоваться как для таргетирования рекламы, так и для злонамеренных действий.

Утечка персональных данных может привести к следующим негативным последствиям:

– финансовые потери – кража денег со счетов, оформление кредитов на имя жертвы;
– репутационный ущерб – разглашение личной или медицинской информации;
– таргетированный фишинг – атаки, учитывающие интересы и привычки конкретного человека;
– шантаж – использование личных данных для вымогательства;

Основным фактором, повышающим риск реализации указанных угроз, является чрезмерное доверие пользователя к сервисам[161].

Для снижения рисков рекомендуется применение комплекса мер технического и организационного характера:

– использование менеджеров паролей (Bitwarden, KeePass);
– включение двухфакторной аутентификации (2FA);
– запрет приложениям необоснованных разрешений;
– использование VPN и блокировщиков трекеров (uBlock Origin);
– регулярная проверка того, какие сервисы имеют доступ к аккаунту;
– отказ от публикации геометок, снимков документов, номеров билетов;
– удаление неиспользуемых учётных записей.

В ходе проведённого анализа установлено:

– 87 % бесплатных приложений запрашивают избыточные разрешения, не связанные с их основной функциональностью;
– более 60 % пользователей не меняют пароли после сообщений об утечках данных;
– штатные защитные механизмы браузеров не блокируют скрытые трекеры;
– шифрование трафика (HTTPS) не защищает от сбора данных на стороне сервера.

---

[160] Шадманов З. З. Цифровая гигиена: важность и лучшие практики. URL: https://cyberleninka.ru/article/n/tsifrovaya-gigiena-vazhnost-i-luchshie-praktiki (дата обращения: 29.03.2026).

[161] Петрова К. А. Защита конфиденциальности данных и прав личности в цифровой среде: правовое регулирование и практические механизмы. URL: https://cyberleninka.ru/ (дата обращения: 29.03.2026).

Таким образом, пользовательская осведомлённость остаётся главным барьером на пути утечки персональных данных.

В результате выполнения работы были выявлены основные каналы утечки персональных данных пользователей в цифровой среде и предложены практические меры защиты. Установлено, что приложения и сайты собирают значительный объём информации о пользователях, часто без их явного ведома. Использование только одного пароля является недостаточным – необходима двухфакторная аутентификация. Пользователям следует критически оценивать запрашиваемые приложениями разрешения и не предоставлять доступ к контактам, камере или геолокации при отсутствии явной необходимости[162].

Главный принцип защиты, сформулированный по итогам работы: минимизировать передаваемые данные, проверять разрешения, использовать двухфакторную аутентификацию и уникальные пароли. Технологические средства защиты являются важным, но не достаточным условием – ключевая роль принадлежит осознанному поведению самого пользователя.

УДК 621.373.421.15(045)

П. Д. Русских, П. П. Андреева,
обучающиеся 2 курса Института права,
социального управления и безопасности ФГБОУ ВО «УдГУ».
Научный руководитель: Т. Н. Стерхова, канд. техн. наук, доцент
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Исследование RC-генератора

Генераторы гармонических сигналов широко востребованы в измерительных приборах, средствах радиосвязи и системах цифровой обработки данных. В отличие от высокочастотных LC-контуров, которые сложно реализовать на инфранизких частотах из-за внушительных габаритов и массы индуктивных элементов, RC-генераторы позволяют получать стабильные колебания в широком диапазоне без применения катушек индуктивности[163]. Отказ от индуктивностей дает возможность миниатюризировать устройство и применять интегральные технологии, однако при этом снижается добротность частотно-задающих цепей, что ухудшает фильтрацию высших гармоник.

Цель настоящей работы – экспериментальное изучение влияния фазо-балансной цепи (ФБЦ) на частоту генерируемого сигнала, анализ работы автоматической регулировки усиления (АРУ) с точки зрения улучшения формы выходного напряжения, а также выявление условий перехода схемы из режима синусоидальной генерации в режим релаксационных колебаний (мультивибратор).

Теоретическая часть. Условия баланса и мост Вина

В качестве объекта исследования выбран RC-генератор на неинвертирующем операционном усилителе (ОУ) с частотно-зависимой положительной обратной связью (ПОС), реализованной на мосте Вина (элементы C1, C2, сдвоенный потенциометр R). Принципиальная схема такого генератора представлена на рис. 1.

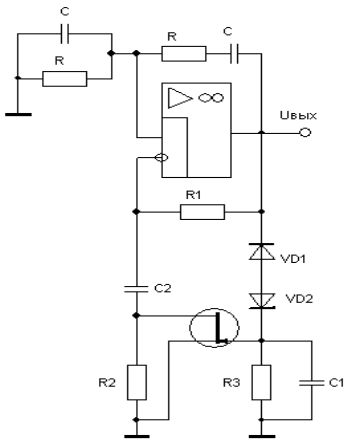


Рис. 1. Схема RC-генератора с мостом Вина

[162] Яппаров Д. Ф. Цифровая гигиена: как защитить свои данные. URL: https://phsreda.com/ (дата обращения: 29.03.2026).
[163] RC-генераторы // StudFiles. URL: https://studfile.net/preview/5468513/page:2/ (дата обращения: 21.04.2026).

Для того чтобы в замкнутой системе возникли устойчивые автоколебания, необходимо одновременное соблюдение двух ключевых условий, известных из теории генераторов:

1. Баланс фаз: суммарный сдвиг фазы по контуру «усилитель – обратная связь» должен составлять 2π (или быть кратным этой величине). Иными словами, сигнал, обойдя замкнутую цепь, возвращается на вход в совпадающей по фазе форме.

2. Баланс амплитуд: произведение коэффициентов передачи усилителя и цепи обратной связи (βK) должно быть не меньше единицы – это позволяет компенсировать потери в пассивной частотно-избирательной цепи за счет активности усилительного элемента[164].

В схеме с мостом Вина фазовый сдвиг ψ_β обращается в ноль на частоте квазирезонанса f_0, которая задается параметрами времязадающей цепи. Если принять $R1 = R2 = R$ и $C1 = C2 = C$, то частота генерации вычисляется по выражению:

$$f_0 = \frac{1}{2\pi RC}$$

На данной частоте коэффициент передачи цепи ПОС равен $\beta = 1/3$. Следовательно, для запуска генерации (выполнения амплитудного условия) неинвертирующий усилитель на ОУ должен обеспечивать коэффициент усиления $K \geq 3$. Чтобы стабилизировать амплитуду и избежать насыщения ОУ (которое приводит к нелинейным искажениям), применяется система автоматической регулировки усиления (АРУ).

Методика и проведение эксперимента

В состав экспериментальной установки входили лабораторный стенд с модулем «ГЕНЕРАТОРЫ», осциллограф, вольтметр переменного напряжения и анализатор спектра на основе ПК.

На первом этапе измерялись параметры разомкнутой системы. На вход ФБЦ подавался сигнал $U_{\text{вх}\beta} = 1$ В от внешнего генератора, настроенного на частоту самогенерации схемы $f_\text{Г}$. Фиксировалось выходное напряжение $U_{\text{вых}\beta}$ и определялся коэффициент передачи β. Ключевым моментом стало экспериментальное нахождение частоты нулевого фазового сдвига f_0: с помощью двухлучевого режима осциллографа частота внешнего сигнала плавно изменялась до тех пор, пока фазы входного и выходного напряжений ФБЦ не совпадали.

Второй этап заключался в сравнении осциллограмм и спектрограмм выходного сигнала при работающей и отключенной АРУ. Оценивалось влияние автоматической регулировки на уровень высших гармоник и стабильность формы колебаний.

Третий этап предполагал перестройку схемы: путем исключения моста Вина из цепи обратной связи и коммутации соответствующих разъемов стенда (в соответствии с инструкцией к лабораторной установке) схема переводилась в режим мультивибратора. Анализировались изменения формы и спектра генерируемого сигнала.

Анализ полученных результатов

В ходе эксперимента были получены количественные данные, хорошо согласующиеся с теоретическими положениями (табл. 1).

Таблица 1

Параметры разомкнутой системы и петлевого усиления

Параметр	Значение
Частота генерации $f_\text{Г}$	4.52 кГц
Выходное напряжение генератора $U_\text{Г}$	2.4 В
Коэффициент усиления ОУ, K	3.15
Коэффициент передачи ФБЦ, β	0.31
Частота нулевого фазового сдвига f_0	4.48 кГц
Петлевое усиление βK	0.98

Полученные результаты демонстрируют хорошую сходимость теории и практики. Экспериментально найденное значение f_0 (4.48 кГц) с учетом погрешности номиналов потенциометров практически совпадает с частотой самогенерации $f_\text{Г}$ (4.52 кГц). Это подтверждает, что автоколебания устанавливаются именно на частоте, где выполняется баланс фаз.

[164] Дьяченко Ю. Н. RC-генератор синусоидальных сигналов: методические указания к лабораторным работам // Электронная библиотека СПбПУ Петра Великого. 2018. URL: https://elib.spbstu.ru/ (дата обращения: 21.04.2026).

Небольшое отклонение петлевого усиления от теоретического порога ($\beta K \approx 0.98$ вместо ≥ 1) связано с погрешностью измерения малых напряжений мультиметром и различием между статическим (разомкнутым) и динамическим (замкнутым) режимами. В реальной схеме в момент запуска коэффициент усиления временно возрастает за счет переходных процессов и шумов, что и инициирует «раскачку» генератора.

Сравнение спектрограмм при выключенной и включенной АРУ наглядно показало эффективность автоматической регулировки. При отключенной АРУ наблюдалось уплощение вершин синусоиды из-за насыщения ОУ, а в спектре появлялась ярко выраженная третья гармоника (коэффициент гармоник $k_г \approx 5 - 10\%$). Включение АРУ позволило удержать амплитуду в линейной зоне характеристики ОУ, получив практически идеальную синусоиду с уровнем гармоник ниже – 40 дБ.

При переходе к конфигурации мультивибратора синусоидальный сигнал трансформировался в релаксационные колебания, близкие к форме меандра. Спектр такого сигнала оказался насыщен нечетными гармониками, а частота колебаний определялась уже не квазирезонансом ФБЦ, а постоянной времени $\tau = RC$ процессов заряда и разряда конденсаторов.

В результате выполненного исследования экспериментально подтверждены основные теоретические положения, касающиеся RC-автогенераторов:

1. Частота генерации в схеме с мостом Вина однозначно задается параметрами частотно-зависимой фазо-балансной цепи и соответствует частоте $f_0 = \frac{1}{2\pi RC}$, при которой фазовый сдвиг в цепи ПОС становится нулевым.
2. Применение системы АРУ является критически важным для получения низкого уровня нелинейных искажений. Без АРУ усилитель входит в насыщение, что искажает форму сигнала и порождает паразитные гармоники.
3. Продемонстрирована возможность трансформации схемы из генератора гармонических сигналов в релаксационный генератор (мультивибратор) путем изменения структуры цепей обратной связи.

УДК 34:004.738.5(045)

М. И. Самсонов,
обучающийся 3 курса Института права,
социального управления и безопасности ФГБОУ ВО «УдГУ».
Научный руководитель: Е. А. Яковлева, ассистент
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Правовой статус VPN-сервисов в условиях цифровой трансформации

Активная цифровизация всех сфер общественной жизни ставит перед правом новые задачи: как обеспечить национальную безопасность в информационном пространстве, не ограничивая при этом законные интересы граждан и бизнеса. Особое место в этой дискуссии занимают VPN-сервисы[165], которые, возникнув как инструмент защиты корпоративных коммуникаций, превратились в массовый потребительский продукт[166].

С технической точки зрения VPN – это технология формирования зашифрованного туннеля между устройством пользователя и удалённым сервером, скрывающая реальный IP-адрес и обеспечивающая конфиденциальность трафика[167]. Именно это свойство порождает правовую коллизию: право гражданина на неприкосновенность частной жизни и свободный доступ к информации, не запрещённой законом, вступает в противоречие с полномочиями государства по обеспечению информационной безопасности[168].

[165] VPN-сервисы (Virtual Private Network) – виртуальные частные сети.

[166] Бачило И. Л. Информационное право : учебник для академ. бакалавриата. 5-е изд., перераб. и доп. М. : Юрайт, 2023. С. 215–218.

[167] Полякова Т. А. Правовое регулирование использования технологий виртуальных частных сетей (VPN) в условиях реализации национальных интересов // Право и государство: теория и практика. 2024. № 2. С. 112.

[168] Конституция Российской Федерации : принята всенародным голосованием 12 декабря 1993 г. (с учётом поправок, внесённых Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 01.07.2020 № 11-ФКЗ) // СЗ РФ. 2014. № 31. Ст. 4398 // СПС «КонсультантПлюс» (дата обращения: 01.04.2026).

Запрос общества на анонимный доступ к информации неуклонно растёт: по данным аналитиков, российская аудитория VPN-пользователей уже исчисляется десятками миллионов человек[169]. Вместе с тем регуляторная среда в данной сфере формируется ускоренными темпами – пакет нормативных актов 2017–2024 гг. создаёт сложный механизм, требующий системного осмысления[170]. Принципиально важен вопрос разграничения: право на информацию[171] должно сосуществовать с требованиями к информационной безопасности государства[172]. Наконец, многообразие национальных подходов к регулированию VPN в разных правовых системах придаёт теме сравнительно-правовое измерение[173].

Российское законодательство не содержит легального определения VPN как технологии, что само по себе осложняет её правовую квалификацию[174]. Технически VPN реализуется посредством совокупности протоколов (OpenVPN, WireGuard, IKEv2 и др.), применяющих криптографические методы туннелирования трафика[175]. Защищённый канал обеспечивает три базовых параметра: конфиденциальность (недоступность содержимого для посторонних), целостность (невозможность незаметного изменения) и аутентификацию (подтверждение подлинности узлов)[176].

С правовой точки зрения VPN можно рассматривать в трёх аспектах:

1) инструмент кибербезопасности организации, направленный на защиту коммерческой тайны и персональных данных при удалённой работе сотрудников;

2) средство обхода государственных блокировок при доступе к ресурсам из реестра запрещённых[177];

3) объект технического регулирования, поскольку организации, предоставляющие VPN-услуги, фактически оказывают услуги связи, подпадающие под требования Федерального закона «О связи»[178].

Примечательно, что прямого запрета на использование VPN в российском законодательстве не установлено; вместе с тем Роскомнадзор наделён полномочиями ограничивать доступ к информации, распространяемой с нарушением закона[179]. Таким образом, складывается правовая основа для регуляторного воздействия на VPN-сервисы как на технологических посредников[180].

Российское законодательство формирует комплексный механизм регулирования, охватывающий как прямые обязательства операторов VPN-сервисов, так и косвенные ограничения для конечных пользователей[181]. Базовый нормативный акт – Федеральный закон «Об информации, информационных технологиях и о защите информации»[182] – предусматривает создание единого реестра запрещённой информации (ст. 15.1) и регламентирует обязанности операторов поисковых систем и владельцев информационных ресурсов (ст. 15.8).

Федеральный закон «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации»[183] наделил Роскомнадзор правом обязывать владельцев VPN-сервисов, анонимайзеров и прокси-серверов подключаться к ФГИС для исполнения требований о блокировке запрещённых ресурсов. Уклонение от подключения влечёт блокировку самого сервиса на территории Российской Федерации.

---

[169] Аналитический отчёт: тенденции использования VPN в России // РБК. 2025. URL: https://www.rbc.ru (дата обращения: 01.04.2026).

[170] О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» : Федеральный закон от 29 июля 2017 г. № 276-ФЗ // СЗ РФ. 2017. № 31 (ч. I). Ст. 4824 // СПС «КонсультантПлюс» (дата обращения: 01.04.2026).

[171] Конституция Российской Федерации : принята всенародным голосованием 12 декабря 1993 г. // СЗ РФ. 2014. № 31. Ст. 4398 // СПС «КонсультантПлюс» (дата обращения: 01.04.2026).

[172] Об утверждении Доктрины информационной безопасности Российской Федерации : Указ Президента РФ от 5 декабря 2016 г. № 646 // СЗ РФ. 2016. № 50. Ст. 7074.

[173] Международный опыт ограничения доступа к информации: страны АТР / под ред. А. В. Фёдорова. М. : Институт развития интернета, 2024. С. 45–67.

[174] Полякова Т. А. Указ. соч. С. 114.

[175] Privacy Affairs. State of VPN in 2025: Global Report. 2025. P. 12.

[176] Forbes Tech. Как работает шифрование в VPN-протоколах. 2024. URL: https://www.forbes.ru (дата обращения: 01.04.2026).

[177] РБК. VPN под запретом? Разбор правоприменительной практики. 2025. URL: https://www.rbc.ru (дата обращения: 01.04.2026).

[178] О связи : Федеральный закон от 7 июля 2003 г. № 126-ФЗ // СЗ РФ. 2003. № 28. Ст. 2895 (дата обращения: 01.04.2026).

[179] Об информации, информационных технологиях и о защите информации : Федеральный закон от 27 июля 2006 г. № 149-ФЗ // СЗ РФ. 2006. № 31 (ч. I). Ст. 3448 (дата обращения: 01.04.2026).

[180] Полякова Т. А. Указ. соч. С. 115.

[181] Там же. С. 116.

[182] Об информации, информационных технологиях и о защите информации : Федеральный закон от 27 июля 2006 г. № 149-ФЗ. Ст. 15.1, 15.8 // СПС «КонсультантПлюс» (дата обращения: 01.04.2026).

[183] О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» : Федеральный закон от 29 июля 2017 г. № 276-ФЗ // СЗ РФ. 2017. № 31 (ч. I). Ст. 4824 (дата обращения: 01.04.2026).

Технический порядок взаимодействия с государственной системой ограничения доступа закреплён ведомственными актами Роскомнадзора[184].

Федеральный закон «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации»[185] предоставил Роскомнадзору полномочия по централизованному управлению сетью связи общего пользования, открыв возможность блокировки «неподконтрольных» VPN-сервисов непосредственно на уровне операторов связи.

Сложившаяся модель регулирования такова: VPN-сервисы, подключившиеся к ФГИС либо не обеспечивающие обход блокировок, функционируют в правомерном режиме; зарубежные же сервисы, игнорирующие требования российского законодательства, подлежат ограничению доступа через операторов связи[186]. Органы государственной власти тем самым выстраивают механизм информационной безопасности в соответствии с национальными и международными стандартами.

По официальной позиции Роскомнадзора и устойчивой правоприменительной практике, само использование VPN состава правонарушения не образует[187]; юридические последствия наступают исключительно за конкретные противоправные действия, совершённые посредством VPN[188].

Для пользователей правовые риски концентрируются в трёх плоскостях:

1) административная ответственность по ст. 13.41 Кодекса Российской Федерации об административных правонарушениях – за распространение информации с ограниченным доступом в случае, если пользователь через VPN посещает запрещённые ресурсы и размещает на них контент;

2) уголовная ответственность по ст. 207.3 (распространение заведомо ложной информации о Вооружённых Силах РФ), ст. 282 (возбуждение ненависти) и ст. 242 (незаконное распространение порнографии) Уголовного кодекса Российской Федерации[189], если соответствующие деяния совершены с применением средств обхода блокировок;

3) гражданско-правовые последствия в трудовых отношениях: использование неавторизованных VPN-каналов может нарушить условия трудового договора о защите служебной или коммерческой тайны в соответствии с положениями Трудового кодекса Российской Федерации[190].

Применительно к владельцам VPN-сервисов и операторам связи законодательство предусматривает:

1) включение в реестр нарушителей авторских и смежных прав при предоставлении доступа к пиратскому контенту[191];

2) блокировку доменных имён и IP-адресов за отказ от подключения к ФГИС согласно ст. 15.8 Федерального закона «Об информации, информационных технологиях и о защите информации»[192];

3) взыскание убытков и оборотных штрафов за создание условий для распространения запрещённой информации[193].

Рассмотрим зарубежный опыт правового регулирования VPN-технологий.

В Китайской Народной Республике действует наиболее жёсткая запретительная модель. С 2018 г. физические лица лишены права пользоваться VPN-сервисами, не прошедшими государственную лицензирование: весь трафик в обязательном порядке проходит через централизованный фильтрационный шлюз «Золотой щит»[194]. Лицензированные каналы VPN допускаются исключительно для использования иностранными компаниями и государственными учреждениями; нарушителям грозят существенные штрафы и блокировка оборудования.

---

[184] Об утверждении Порядка взаимодействия операторов поисковых систем с федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации : приказ Роскомнадзора от 21 ноября 2017 г. № 185 // СПС «КонсультантПлюс» (дата обращения: 01.04.2026).

[185] О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации» : Федеральный закон от 1 мая 2019 г. № 90-ФЗ // СЗ РФ. 2019. № 18. Ст. 2214 (дата обращения: 01.04.2026).

[186] Аналитический отчёт: тенденции использования VPN в России. Указ. соч. С. 8.

[187] О применении мер ограничения доступа к VPN-сервисам : разъяснения Роскомнадзора от 15 марта 2024 г. // Официальный сайт Роскомнадзора. URL: https://rkn.gov.ru (дата обращения: 01.04.2026).

[188] Кодекс Российской Федерации об административных правонарушениях : Федеральный закон от 30.12.2001 № 195-ФЗ (ред. от 28.04.2025) // СЗ РФ. 2002. № 1 (ч. I). Ст. 1 (дата обращения: 01.04.2026).

[189] Уголовный кодекс Российской Федерации : Федеральный закон от 13 июня 1996 г. № 63-ФЗ (ред. от 28.04.2025). Ст. 207.3, 282, 242 // СЗ РФ. 1996. № 25. Ст. 2954 (дата обращения: 01.04.2026).

[190] Трудовой кодекс Российской Федерации : Федеральный закон от 30 декабря 2001 г. № 197-ФЗ (ред. от 28.04.2025) // СЗ РФ. 2002. № 1 (ч. I). Ст. 3 (дата обращения: 01.04.2026).

[191] Лента.ру. VPN-сервисы попали в реестр нарушителей авторских прав. 2025. URL: https://lenta.ru (дата обращения: 01.04.2026).

[192] Об информации, информационных технологиях и о защите информации : Федеральный закон от 27 июля 2006 г. № 149-ФЗ. Ст. 15.8 // СПС «КонсультантПлюс» (дата обращения: 01.04.2026).

[193] Полякова Т. А. Указ. соч. С. 117.

[194] Там же. С. 117.

Государства – члены Европейского союза придерживаются принципиально иного подхода, отдавая приоритет защите основных прав. Регламент GDPR[195] косвенно стимулирует применение шифрования в целях охраны персональных данных. Использование VPN не ограничивается, однако провайдеры подпадают под действие требований о хранении данных (Директива об электронной конфиденциальности) и обязаны оказывать содействие правоохранительным органам при расследовании тяжких преступлений[196].

Соединённые Штаты Америки не располагают единым федеральным законом о VPN. Регулирование осуществляется через отраслевое законодательство о кибербезопасности, а также через надзорные полномочия Федеральной торговой комиссии, преследующей сервисы за вводящие в заблуждение заявления об анонимности и защите данных[197].

Применительно к Российской Федерации можно выделить следующие направления развития правового регулирования VPN-сервисов:

1) разработка специального правового режима для «доверенных» VPN-сервисов российских операторов, встроенных в национальную инфраструктуру защиты информации[198];

2) развитие международного сотрудничества в рамках ООН[199] по продвижению концепции ответственного поведения государств в цифровой среде, что может повлечь унификацию подходов в рамках СНГ, ОДКБ и БРИКС[200];

3) введение дифференцированной ответственности для пользователей и операторов за систематическое применение VPN в целях доступа к ресурсам, внесённым в реестр запрещённых.

Правовой статус VPN-сервисов в Российской Федерации находится в состоянии активного нормативного формирования. Сегодня VPN остаётся законным инструментом, применимым как для защиты правомерных интересов граждан и организаций (безопасность финансовых операций, дистанционная работа с корпоративными ресурсами), так и потенциально – для обхода законодательно установленных ограничений[201].

Дальнейшее правовое развитие, по всей видимости, будет ориентировано не на запрет самой технологии, а на выстраивание регулируемой среды, в которой операторы, владельцы сервисов и пользователи несут соразмерную ответственность за нарушение установленных запретов. Ключевым вызовом для законодателя и правоприменителя останется поиск устойчивого баланса между правом на частную жизнь и задачами противодействия угрозам в цифровом пространстве[202].

УДК 004.35(045)

М. П. Саранчин,

обучающийся 2 курса Института права,
социального управления и безопасности ФГБОУ ВО «УдГУ».
Научный руководитель: О. В. Меркушев, канд. техн. наук, доцент
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Основные подходы к восстановлению данных на блочных устройствах

В современных информационных системах данные являются одним из наиболее ценных ресурсов, их сохранность напрямую влияет на непрерывность работы организаций и удобство повседневной деятельности пользователей. В большинстве случаев, данные хранятся на блочных устройствах[203] в файловых системах – при высокой надёжности этих устройств, риск потери данных не исключен, он может быть связан с аппаратными сбоями или ошибками пользователя.

---

[195] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation). OJ L 119, 04.05.2016. P. 1–88.

[196] Международный опыт ограничения доступа к информации: страны АТР / под ред. А. В. Фёдорова. Указ. соч. С. 102–108.

[197] Federal Trade Commission. VPN Services: What They Say vs. What They Do. 2024. URL: https://www.ftc.gov (дата обращения: 01.04.2026).

[198] Бачило И. Л. Указ. соч. С. 222.

[199] ООН. Открытая рабочая группа по вопросам безопасности в сфере использования информационно-коммуникационных технологий. Итоговый доклад. 2021. URL: https://www.un.org (дата обращения: 01.04.2026).

[200] Международный опыт ограничения доступа к информации: страны АТР / под ред. А. В. Фёдорова. Указ. соч. С. 130.

[201] Бачило И. Л. Указ. соч. С. 225.

[202] Полякова Т. А. Указ. соч. С. 120.

[203] Red Hat. Block Device Guide // Red Hat Documentation. URL: https://docs.redhat.com/ (дата обращения: 25.04.2026).

Цель моей работы – изучить известные методы восстановления данных на блочных устройствах и выбрать наиболее эффективные подходы.

Блочное устройство – это тип устройства ввода-вывода, которое позволяет читать и записывать данные фиксированными порциями – блоками. Блоки имеют свой адрес, по которым система может к ним обращаться. Файловая система – это слой абстракции между «сырыми» блоками устройства и файлами, понятными пользователю.

Аппаратные средства. Программно-аппаратный комплекс PC-3000 – это профессиональное решение от компании ACELab для диагностики, ремонта и восстановления данных с жестких дисков (HDD), твердотельных накопителей (SSD) и других устройств хранения информации. Комплекс широко используется в центрах восстановления данных и лабораториях компьютерной криминалистики по всему миру.

Основные возможности:

- Диагностика и ремонт HDD/SSD с интерфейсами SATA, PATA (IDE), SAS, SCSI, USB, M.2, NVMe.
- Восстановление данных с логически и физически поврежденных накопителей, включая работу с зашифрованными и виртуальными дисками (Bitlocker, VMDK, VHDX и др.).
- Работа в технологическом режиме: исправление программных модулей, отключение неисправных головок, блокировка поврежденных участков, восстановление служебной информации.
- База данных ресурсов: образы Flash ROM, модули служебной информации, треки служебной зоны для работы с поврежденными дисками[204].

Метаданные файловой системы. Почти все широко используемые файловые системы в современных ИС имеет схожую структуру метаданных. Для восстановления с использованием метаданных необходимо обратить внимание на записи директорий и связи файлов с блоками данных. Последняя связь обеспечивается либо с помощью группы указателей (к каждому блоку данных свой указатель, например, как в ext3) или с помощью структуры, называемой extent (ext4, ntfs). Extent имеет указатель на первый блок данных и длинну в виде количества смежных блоков. Таблица директории хранит информацию о пути к файлу и названию. Таким образом, прочитав информацию о метаданных файла можно скопировать блоки данных и провести восстановление. Тем не менее, это один из самых сложных способов, потому что связь метаданных с файлами стирается при перезаписи Inode или записи MFT. Чем позже был удалён файл, тем меньше вероятность его восстановить.

Преимущества: высокая надёжность.

Недостатки: невозможность восстановления при утере связи с блоками.

Журнал файловой системы + copy on write. Журнал файловой системы ведёт учёт операций с файлами: запись, удаление, перемещение, замена inode[205]. Журнал файловой системы работает в режиме транзакций, то есть записанная операция должна гарантированно завершиться или не завершиться вообще. Системно журнал используется для восстановления ФС и файлов при ошибках системы, и записи журнала перезаписываются, когда становятся устаревшими, но не удаляются мгновенно. Это позволяет прочитать информацию об изменениях и получить сведения об удалении файлов.

Преимущества: возможность восстановления при сбоях системы.

Недостатки: быстрая перезапись журнала.

Copy-on-write – архитектурная особенность некоторых ФС (btrfs): при записи файла, модификации ФС создаёт копию блоков данных в другом месте и меняет указатель на данные. Таким образом сохраняется старая копия данных.

File carving. Техника восстановления файлов, которая полагается не на метаданные, а на структуру самих данных. Существуют типы файлов, для которых характерны специальные заголовки и окончания файлов. Специальные программы способны находить такие конструкции и выделять данные между ними, таким образом «вырезая» файл из общего объёма данных[206]. Трудности представляют фрагментированные файлы, но существуют программы, которые могут разрешать фрагментацию и выделять полный файл.

Преимущества: независимость от метаданных, высокая вероятность успеха.

Недостатки: требуется анализ всего образа диска полностью.

---

[204] ACELab. PC-3000 UDMA [Электронный ресурс] // ACELab. URL: https://www.acelab.ru/dep.pc/pc3000udma.php (дата обращения: 25.04.2026).

[205] The kernel development community. 3.6. Journal (jbd2) // The Linux Kernel. URL: https://www.kernel.org/doc/html/latest/filesystems/ext4/journal.html (дата обращения: 25.04.2026).

[206] Forensics Community. File Carving // Forensics Wiki. URL: https://forensics.wiki/file_carving/ (дата обращения: 25.04.2026).

DLP. Данный класс решений осуществляет контроль за работой сотрудников с защищаемой информацией, за потоками конфиденциальных данных в инфраструктуре компании и способами их обработки. Не является методом восстановления, но позволяет предотвратить потерю данных. Data Loss Prevention – система, которая в активном режиме отслеживает все операции с файлами в системе. На основе анализа поведения выявляет случаи, в которых информация может быть потеряна по неосторожности и предотвращает утерю данных. С помощью регулярных выражений система способна выявлять файлы, которые, вероятнее всего, не должны быть удалены и ставит на них соответствующий флаг[207].

Преимущества: защита в реальном времени.

Недостатки: ложные срабатывания, замедление работы, не позволяет восстановить уже удалённые файлы.

Внедрение искусственного интеллекта. Самые распространённые решения в мире ИИ для восстановления является разработками для обнаружения испорченных секторов и устранения этих ошибок. Тем не менее существуют решения, которые встраиваются в предыдущие методы для оптимизации и повышения эффективности[208].

Преимущества: высокая скорость.

Недостатки: вероятность ложных срабатываний и артефактов.

Резервное копирование. Резервное копирование – это заблаговременное создание копии как определённых данных, так и самой системы. Является наиболее эффективным, потому что полностью гарантирует целостность данных в неизменном виде при правильном хранении копии. Одна из наиболее популярных стратегий: 3-2-1 – 3 копии данных на 2 разных типах носителей, 1 копия вне помещения.

Преимущества: гарантированное восстановление.

Недостатки: необходимость актуализировать резервную копию.

Методы, основанные на метаданных, дают наиболее точный результат, но полностью зависят от их сохранности. Журналы файловых систем и copy-on-write эффективны только для недавних изменений. При потере структуры данных применяются сигнатурные методы, такие как file carving, которые более универсальны, но менее точны. Аппаратные решения незаменимы при физических повреждениях, однако требуют значительных ресурсов.

При этом единственным способом, гарантирующим восстановление данных, остаётся резервное копирование.

Таким образом, надёжная стратегия работы с данными – это всегда комбинация превентивных мер и методов восстановления, применяемых в зависимости от конкретного сценария потери.

УДК 621.316.9:004(045)

К. В. Соловьева,
обучающаяся 2 курса Института права,
социального управления и безопасности ФГБОУ ВО «УдГУ».
Научный руководитель: Т. Н. Стерхова, канд. техн. наук, доцент
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Выявление побочных электромагнитных излучений блока питания релейной защиты методом резонансного анализа с помощью параллельного колебательного контура

Микропроцессорные устройства релейной защиты и автоматики (РЗА) взаимодействуют с важной для энергосистемы информацией. Эти устройства относят к элементам критической информационной инфраструктуры. С переходом на цифровые технологии появилась новая угроза: может происходить утечка данных по техническим каналам, в том числе через побочные электромагнитные излучения и наводки (ПЭМИН). Любое электронное устройство создает паразитные электромагнитные поля,

[207] Рахметов Р. DLP системы (Data Loss Prevention, ДЛП) – что это такое // Security Vision. URL: https://www.securityvision.ru/blog/chto-takoe-dlp-sistemy-i-kak-oni-primenyayutsya/ (дата обращения: 25.04.2026).

[208] Russell Chozick. The Role of Artificial Intelligence in Data Recovery // flashback data. URL: https://www.flashback-data.com/ai-data-recovery/ (дата обращения: 25.04.2026).

которые иногда можно зафиксировать даже за пределами контролируемой зоны. А для объектов электроэнергетики, где полноценное экранирование затруднено, это очень серьезная проблема.

Цель этой работы – разработать простой и недорогой способ обнаружения ПЭМИН от блоков питания устройств РЗА.

1. Анализ угроз утечки информации по каналам ПЭМИН.

В устройствах релейной защиты и автоматики побочные электромагнитные излучения и наводки могут исходить от разных устройств:

- тактовые генераторы микроконтроллеров и цифровых сигнальные процессоров;
- импульсные блоки питания;
- кабельные линии интерфейсов;
- неэкранированные корпуса и монтажные платы.

Перехват паразитного излучения блока питания позволяет злоумышленнику определить моменты срабатывания защиты и даже тип аварии, что создаёт предпосылки для целенаправленных кибератак[209]. Существующие методы защиты (экранирование, фильтрация, заземление) затратны и не всегда применимы на действующих подстанциях. Поэтому актуальной задачей является разработка простых средств обнаружения факта наличия ПЭМИН, позволяющих персоналу ИБ оперативно оценивать электромагнитную обстановку.

2. Теоретическое обоснование метода резонансного анализа.

В основе предлагаемого метода лежит явление резонанса токов, возникающее в параллельном колебательном контуре. Такой контур, состоящий из катушки индуктивности L и конденсатора C, обладает свойством: на своей резонансной частоте его полное сопротивление становится максимальным и чисто активным[210]. Резонансная частота определяется формулой Томсона:

$$f_0 = \frac{1}{(2\pi\sqrt{LC})}$$

Изменяя ёмкость конденсатора (или индуктивность катушки), можно перестраивать резонансную частоту в некотором диапазоне. Если на такую частоту попадает какая-либо спектральная составляющая ПЭМИН от исследуемого устройства, напряжение на контуре резко возрастает. Таким образом, параллельный колебательный контур с переменной ёмкостью может работать как простейший узкополосный анализатор спектра. Для преобразования высокочастотного напряжения, выделенного контуром, в сигнал, удобный для визуального наблюдения, используется амплитудный етектор (диод и RC-фильтр). Такой подход является классическим для радиоприёмной техники и отличается простотой и надёжностью.

3. Принципиальная схема индикатора ПЭМИН.

На основе описанного метода была разработана принципиальная схема индикатора ПЭМИН (рис. 1).

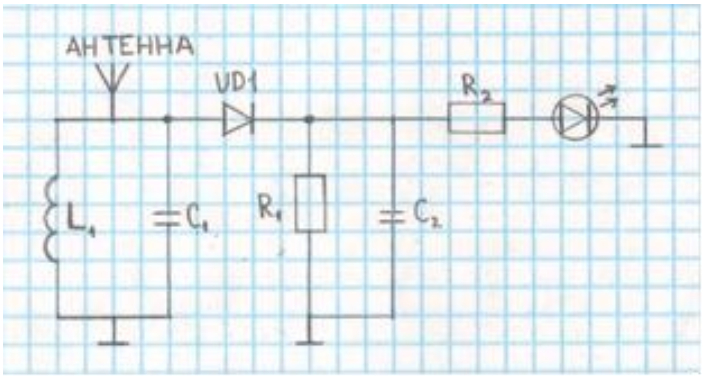


Рис. 1. Принципиальная электрическая схема индикатора ПЭМИН
на основе параллельного колебательного контура

Устройство состоит из следующих функциональных блоков:

1. Входная цепь (антенна). В качестве антенны может использоваться короткий отрезок провода (10–20 см) или ферритовая магнитная антенна, в зависимости от диапазона частот.

[209] Об утверждении дополнительных требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры, функционирующих в сфере электроэнергетики : приказ Минэнерго России от 26.12.2023 № 1215.

[210] Зернов Н. В., Карпов В. Г. Теория радиотехнических цепей. Л. : Энергия, 1972. 816 с.

2. Перестраиваемый параллельный колебательный контур. Образован катушкой индуктивности L1 (например, 5–10 витков медного провода диаметром 0,5 мм на оправке 10 мм) и конденсатором переменной ёмкости C1 (типа КП-180, диапазон 10–150 пФ).

3. Амплитудный детектор. Выполнен на высокочастотном диоде VD1 (например, 1N4148 или КД522) и RC-фильтре, состоящем из резистора R1 (10–100 кОм) и конденсатора C2 (1–10 нФ).

4. Усилитель постоянного тока (опционально). Для повышения чувствительности после детектора может быть включён неинвертирующий усилитель на операционном усилителе (например, LM358), однако в простейшем варианте можно обойтись без него.

5. Индикаторное устройство. В качестве индикатора может использоваться светодиод HL1 с ограничительным резистором R2 (300–500 Ом) или стрелочный микроамперметр на 50–100 мкА.

Принцип работы устройства. Электромагнитное поле, создаваемое блоком питания исследуемого терминала РЗА, наводит высокочастотное напряжение на антенне и на элементах колебательного контура L1, C1. Оператор вращает ротор переменного конденсатора C1, изменяя резонансную частоту контура. В тот момент, когда эта частота совпадает с частотой какой-либо спектральной составляющей ПЭМИН, на контуре возникает максимальное напряжение. Это напряжение поступает на диод VD1, который выпрямляет высокочастотный сигнал. RC-фильтр R1, C2 сглаживает пульсации, и на выходе детектора образуется постоянное напряжение, пропорциональное амплитуде принятого сигнала. Это напряжение (через усилитель, если он используется) подаётся на индикатор – светодиод загорается, стрелка микроамперметра отклоняется. По яркости свечения или углу отклонения стрелки можно судить об относительной интенсивности излучения на данной частоте.

4. Порядок применения и возможные режимы работы. Для выявления ПЭМИН от блока питания устройства РЗА предлагается следующий порядок действий:

1) индикатор подносится к исследуемому блоку питания на расстояние 0,2–0,5 м;

2) плавно вращая ротор конденсатора переменной ёмкости C1, оператор наблюдает за индикатором;

3) в момент настройки на частоту, совпадающую с одной из гармоник тактового генератора или шумов импульсного преобразователя, индикатор фиксирует максимум (светодиод вспыхивает ярче, стрелка отклоняется);

4) отметив несколько таких максимумов, можно получить представление о частотных диапазонах, в которых блок питания создаёт наиболее интенсивные излучения. Устройство может работать в двух основных режимах:

- режим поиска (сканирования). Оператор медленно перестраивает контур во всём рабочем диапазоне частот, выявляя наличие излучений;
- режим мониторинга. Индикатор фиксируется на определённой частоте (например, на частоте тактового генератора), и по изменению яркости свечения можно судить о стабильности уровня излучения во времени.

5. Достоинства и ограничения метода. Предлагаемый метод и устройство на его основе имеют следующие достоинства:

- Низкая стоимость. Все компоненты (катушка, переменный конденсатор, диод, резисторы, светодиод) являются общедоступными и стоят не более 500 рублей.
- Простота изготовления**.** Устройство может быть собрано за один час в любой электролаборатории без специального оборудования.
- Наглядность. Индикация в виде свечения светодиода или отклонения стрелки не требует специальных знаний для интерпретации.
- Автономность. В пассивном варианте (без усилителя) устройство не требует питания.

Ограничения метода связаны с его невысокая чувствительность и избирательность по сравнению с профессиональными анализаторами спектра. Тем не менее, для оперативного контроля электромагнитной обстановки и выявления аномально высоких уровней ПЭМИН возможностей достаточно.

В ходе выполнения работы был разработан простой метод обнаружения побочных электромагнитных излучений блоков питания устройств РЗА на основе резонансного анализа с помощью параллельного колебательного контура. Предложена принципиальная схема индикатора, описан принцип действия. Устройство может применяться службами информационной безопасности объектов электроэнергетики для экспресс-оценки электромагнитной обстановки, выявления блоков питания с повышенным уровнем ПЭМИН, обнаружения несанкционированных радиозакладок и сравнительных испытаний оборудования. Перспективными направлениями являются повышение чувствительности и автоматизация сканирования с использованием микроконтроллера.

УДК 621.375.026(045)

И. М. Сухов,
обучающийся 4 курса Института права,
социального управления и безопасности ФГБОУ ВО «УдГУ».
Научный руководитель: Т. Н. Стерхова, канд. техн. наук, доцент
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Исследование усилителя мощности звуковых частот

Усилители мощности звуковых частот являются ключевыми элементами современной бытовой и профессиональной аудиотехники, систем звуковоспроизведения и измерительных комплексов[211]. Основное назначение таких устройств заключается в повышении мощности входного сигнала до уровня, необходимого для эффективного возбуждения низкоомной нагрузки (акустических систем), при минимальном уровне нелинейных искажений и широкой полосе пропускания. Современные требования к качеству звуковоспроизведения обуславливают необходимость применения многокаскадных схем с глубокой отрицательной обратной связью и тщательным выбором режимов работы активных компонентов.

Целью данной работы является исследование принципа работы усилителя мощности звуковой частоты, приобретение практических навыков моделирования радиосхем в среде Micro-Cap, анализ частотных и амплитудных характеристик, а также оценка коэффициента гармоник и устойчивости схемы.

Усилитель представляет собой электронное устройство, предназначенное для увеличения мощности, напряжения или тока входного сигнала без существенного изменения его формы. Ключевой принцип работы усилителя заключается в том, что он не создаёт энергию самостоятельно, а использует энергию источника питания для формирования усиленной копии входного сигнала[212].

Основные параметры усилителей включают коэффициент усиления по напряжению, току и мощности, входное и выходное сопротивления, полосу пропускания, коэффициент гармоник и коэффициент полезного действия. В зависимости от диапазона усиливаемых сигналов выделяют усилители постоянного тока, низкой частоты (УНЧ), высокой частоты и СВЧ-усилители[213]. Усилители мощности звуковых частот относятся к классу УНЧ и работают в диапазоне 20 Гц…20 кГц.

Важнейшим элементом современных усилителей является отрицательная обратная связь (ООС), при которой часть выходного сигнала возвращается на вход в противофазе. Применение ООС приводит к снижению коэффициента усиления, но значительно повышает стабильность работы, расширяет полосу пропускания и уменьшает нелинейные искажения[214]. Положительная обратная связь, напротив, применяется преимущественно в генераторах и триггерных схемах.

Рассматриваемая в работе схема представляет собой трёхкаскадный усилитель мощности:

- входной дифференциальный усилительный каскад на транзисторах VT2, VT3 с динамической нагрузкой в виде токового зеркала (VT4, VT5) и задающим эмиттерным источником тока на элементах VT1, R3, R4, R5;
- промежуточный каскад усиления на составном транзисторе VT6, VT8 по схеме с общим эмиттером, содержащий элемент местной обратной связи по току R13 и источник тока в коллекторной цепи;
- выходной двухтактный каскад на транзисторах разной проводимости VT10, VT11, включённых по схеме комплементарного эмиттерного повторителя, с источником смещения на VT9, R11, R12, обеспечивающим работу в классе АВ.

Дополнительно в схеме применяются входной резисторный делитель R1, R2 для установки постоянного потенциала на выходе на уровне половины напряжения питания, разделительный конденсатор C1, цепь общей отрицательной обратной связи R8, R9, C2 (параллельная по выходу, последовательная по входу), а также резисторы R14, R15 для термостабилизации тока покоя выходных транзисторов[215].

Для практической реализации исследования использовался интерактивный эмулятор радиосхем Micro-Cap, позволяющий проводить анализ переходных процессов, частотных характеристик и нелинейных искажений без изготовления физического макета.

---

[211] Титов В. С., Красько А. А. Электронные устройства: учебник для вузов. М. : Высш. школа, 2018. С. 432.
[212] Степененко И. П. Основы теории усилительных устройств. 4-е изд. М. : Радио и связь, 1990. С. 304.
[213] Гутников В. С. Интегральная электроника в измерительных устройствах. 2-е изд. Л. : Энергоатомиздат, 1988. С. 288.
[214] Бондарев А. Н., Калачёв Б. Н. Теоретические основы электроники. СПб. : СПбГЭТУ «ЛЭТИ», 2015. С. 312.
[215] Руководство пользователя Micro-Cap 12. Spectrum Software, 2021. URL: https://www.spectrum-soft.com (дата обращения: 15.10.2024).

Исходные данные для моделирования:

- сопротивление источника сигнала Rг = 10 кОм;
- эффективное напряжение источника Uг = 3 В;
- требуемая выходная мощность Рвых = 50 Вт;
- сопротивление нагрузки Rн = 8 Ом;
- рабочий частотный диапазон Δf = 300…100 000 Гц;
- напряжение питания Uп = ±35 В.

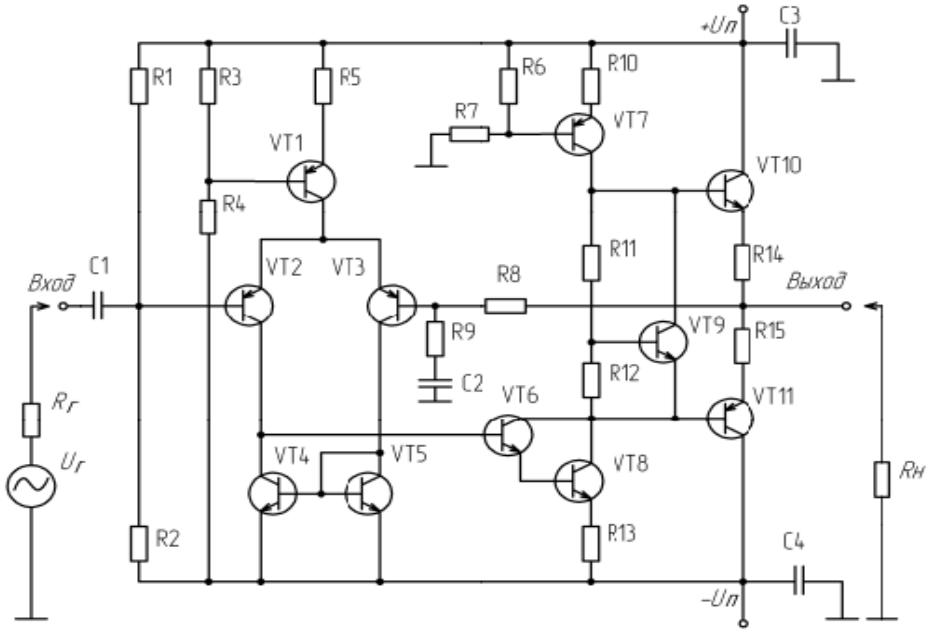


Рис. 1.1. **Усилитель мощности звуковых частот. Схема электрическая принципиальная**

Схема была собрана в соответствии с принципиальной электрической схемой усилителя (см. рис. 1.1[216]). В качестве активных компонентов использовались биполярные транзисторы: VT1 – BC557A, VT2, VT3 – BC560C, VT4 – BC557B, VT5 – BC547B, VT6 – BC547A, VT7 – BC557B, VT8 – MJE350, VT9 – BC557B, VT10, VT11 – комплементарная пара выходных транзисторов[217].

Для анализа переходных процессов применялся инструмент Analysis → Transient. Временной интервал симуляции был установлен с учётом периода низкочастотного сигнала, что позволило наблюдать форму входного и выходного напряжений на осциллограмме. Для получения амплитудно-частотной характеристики использовался режим Analysis → AC с логарифмической развёрткой по частоте в диапазоне от 10 Гц до 1 МГц.

По результатам моделирования установлено, что усилитель обеспечивает стабильное усиление сигнала в заданном рабочем диапазоне частот. АЧХ демонстрирует спад на низких частотах, обусловленный влиянием разделительных конденсаторов C1 и C2, и на высоких частотах, определяемый ёмкостями переходов транзисторов и паразитными монтажами. В пределах полосы пропускания 300…100 000 Гц неравномерность усиления не превышает 3 дБ, что соответствует требованиям к усилителям звуковых частот[218].

Амплитудная характеристика показала линейный участок усиления до достижения напряжения насыщения выходного каскада. При подаче синусоидального сигнала амплитудой 3 В на выходе наблюдается сигнал с коэффициентом усиления, соответствующим заданной выходной мощности 50 Вт на нагрузке 8 Ом. Форма выходного сигнала сохраняет синусоидальность, что свидетельствует о низком уровне гармонических искажений в рабочем режиме.

Применение общей отрицательной обратной связи позволило стабилизировать коэффициент усиления, снизить зависимость параметров схемы от разброса характеристик транзисторов и температуры окружающей среды. В эмиттерных цепях выходных каскадов установлены резисторы R14

---

[216] Расчёт усилителей мощности звуковых частот. Методические указания к выполнению расчетно-графических работ. Омск : Изд-во ОмГТУ, 2012. С. 5.

[217] ГОСТ Р 7.0.5-2008. Система стандартов по информации, библиотечному и издательскому делу. Библиографическая ссылка. Общие требования и правила составления. М. : Стандартинформ, 2008. С. 32.

[218] Хоровиц П., Хилл У. Искусство схемотехники. 3-е изд. М. : Мир, 2020. Т. 1. С. 528.

и R15. За счёт них создаётся местная обратная связь по току, которая автоматически ограничивает рост коллекторного тока при прогреве полупроводников. Такая схемотехническая мера надёжно защищает транзисторы от теплового разгона, даже если рабочая температура поднимается в пределах от +10 до +30 °C.

Проверку на устойчивость проводили, анализируя поведение амплитудно-частотной характеристики на верхних частотах и форму переходного процесса. Полученные графики не выявили признаков самовозбуждения. Корректирующий конденсатор C2, включённый в цепь общей обратной связи, вносит необходимую частотную коррекцию, формируя фазовый запас, который гарантирует стабильное усиление даже при подключении нагрузки с выраженной реактивной составляющей.

Практическая часть исследования базировалась на компьютерном моделировании трёхкаскадного УМЗЧ в среде Micro-Cap. Расчётные соотношения для дифференциального входа, промежуточного каскада усиления напряжения и выходного эмиттерного повторителя класса AB полностью оправдали себя в симуляции. По результатам расчётов устройство развивает мощность 50 Вт на эквиваленте акустической системы (8 Ом), сохраняет равномерное усиление в полосе 300–100 000 Гц и корректно функционирует при симметричном питании ±35 В.

Глубокая отрицательная обратная связь, организованная параллельно по выходу и последовательно по входу, решает сразу несколько задач: согласовывает высокоомный вход с источником сигнала, снижает уровень гармоник и компенсирует температурные дрейфы параметров полупроводников. В целом, выбранная топология доказала свою надёжность в расчётах и может служить базой при разработке как любительских, так и профессиональных аудиоусилителей.

УДК [004.89:316.6]:004.056(045)

В. А. Фёдоров,
обучающийся 2 курса Института права,
социального управления и безопасности ФГБОУ ВО «УдГУ».
Научный руководитель: Е. А. Яковлева, ассистент
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Человеческий фактор 2.0: как deepfake и социальная инженерия ломают MFA

В эпоху цифровой трансформации многопользовательские системы безопасности (например, многофакторная аутентификация, MFA) становятся основой для стандартизации информационной безопасности, ориентированные на развитие и внедрение цифровых технологий в информационное общество. Одним из приоритетных направлений являются технологии искусственного интеллекта. Развитие технологий искусственного интеллекта и методов социальной инженерии существенно увеличивает возникновение информационных угроз. В связи с этим необходимо рассмотреть традиционные подходы к MFA, имеющие уязвимости перед новыми вызовами информационной безопасности.

Актуальность технологий искусственного интеллекта напрямую связана с информационно-психологической угрозой социальной инженерией, которая представляет собой совокупность методов и тактик воздействия, основанных на психологическом манипулировании, с целью контроля поведения человека и доступа к конфиденциальной информации[219].

Искусственный интеллект – комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека. Комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру (в том числе информационные системы, информационно-телекоммуникационные сети, иные технические средства обработки информации), программное обеспечение (в том числе в котором используются методы машинного обучения), процессы и сервисы по обработке данных и поиску решений[220].

[219] Что такое социальная инженерия и чем она опасна. Методы мошенников и способы защиты от них // РБК Life. URL: https://www.rbc.ru/life/news/67697c5d9a794759cf255043?ysclid=mpbkzhmbbx13575007 (дата обращения: 14.05.2026).

[220] О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте… // Федеральный закон от 24.04.2020 № 123-ФЗ. URL: https://www.consultant.ru/ (дата обращения: 20.04.2026).

Использование вышеупомянутых технологий, применяя которые злоумышленник совершает кибер-атаки на объекты становится угрозой нового уровня и как подмечают аналитики: «Социальная инженерия в виде дипфейков и искусного фишинга вышла на новый уровень, поэтому как никогда актуальны программы ИБ-обучения персонала»[221].

В нынешнее время deepfake-технологии применяются для создания высокого уровня реалистичности фальшивых видео и звонков. Злоумышленники в области социальной инженерии сочетают что старые схемы мошенничества, вроде фишинга, или кражи SIM, с новыми технологиями. Особенно актуальны эти угрозы для органов публичной власти, банковской сферы и иных учреждений.

При этом существует проблема защиты от информационных угроз, таких как дипфейки и обход MFA, которая требует особого внимания и поиска современных правовых и организационно-технических мер защиты.

Так, техническим решением является многофакторная аутентификация (Multi-Factor Authentication, MFA), направленная на повышение кибербезопасности и включающая несколько уровней проверки безопасности, прежде чем пользователю будет предоставлен доступ к определенной системе[222]:

1) знание (пароль, PIN-код);
2) владение (SIM-карта, аппаратный токен, смартфон) и
3) свойство (биометрия: голос, лицо, отпечаток).

Дополнительно можно выделить местоположение, определяемое в системах с «нулевым доверием». Zero Trust – «это набор идей и концепций, призванных уменьшить неопределенность в процессе выработки решений по предоставлению минимально необходимых привилегий доступа для каждого поступающего запроса на доступ в информационной системе, исходя из возможности компрометации сети»[223]. Так, механизм MFA чаще всего определяется через Zero Trust, где создается дополнительный барьер для злоумышленника, пытающийся совершить информационную угрозу.

Вместе с тем к распространенным методам, повышающим неопределенность сети, являются: отправка одноразового пароля (OTP) по SMS и электронной почте, push-уведомление на смартфон, приложения-аутентификаторы или биометрия. Каждый из этих методов имеет свои особенности: так, SMS/почта и звонки просты, но подвержены перехвату, TOTP считается более защищённым, а биометрия удобна, но требует защиты шаблонов.

Так, например, Deepfake представляет собой информационную угрозу, реально существующую и актуальную на сегодняшний день. Deepfake получил быстрое развитие, направленное на деструктуризацию общества в целом. Мошенники используют передовые технологии копирования голоса и видео с помощью искусственного интеллекта, с целью нанесения вероятного ущерба.

Подобного уровня угрозы оказывают негативное влияние на информационное общество, повышая общественную опасность для государства в целом. Данная угроза имеет следующие характеристики: реалистичность, упрощенность в механизме управления, минимальная защищенность, где технологии искусственного интеллекта представляют собой потенциальную угрозу и как утверждают Н. Ф. Бодро и А. К. Лебедева: «проч.). Дипфейки могут использоваться для создания фейковых новостей, шантажа, манипулирования общественным мнением, создания высокореалистичных поддельных доказательств»[224]. В связи с этим необходим точечный механизм воздействия, направленная на устранение недостатков, среди которых отмечается многофакторная аутентификация.

Для информационной безопасности MFA является высоким уровнем защищенности данных. Однако при использовании MFA необходимо руководствоваться выбором методов, рассмотренных выше. Вместе с этим требуется их профессиональная оценка, включающая в себя тестирование на скорость выполнения, применение дополнительного оборудования, совместимость процессов и продуктов.

Полагаем, для обеспечения информационной безопасности, разработать Организационный кодекс, который будет включать в себя определённыеправила поведения, позволяющие уменьшить возможные риски, кражи данных и несанкционированный доступ к информации ограниченного

[221] Прогноз развития киберугроз и средств защиты информации – 2026 // R-Vision. URL: https://www.anti-malware.ru/analytics/Technology_Analysis/Cyber-Threat-and-Information-Security-Forecast-2026 (дата обращения: 19.05.2026).

[222] Что такое многофакторная аутентификация? // Kaspersky URL: https://www.kaspersky.ru/resource-center/preemptive-safety/multi-factor-authentication?ysclid=mpbld56sui700261107 (дата обращения: 20.04.2026).

[223] NIST Special Publication 800-207, August 2020 // Stu Mitchell Stu2Labs Stafford, VA. URL: https://doi.org/10.6028/NIST.SP.800-207 (дата обращения: 20.04.2026).

[224] Бодров Н. Ф., Лебедева А. К. Судебно-экспертное противодействие дипфейк-дезинформации // Союз криминалистов и криминологов. 2024. № 4. С. 129–142.

доступа. Организационный кодекс необходимо разрабатывать в соответствии с действующим законодательством[225] и требованиями технических документов[226].

Также необходимо проводить Обучение с новизной: «Симуляция дипфейка». Традиционные тренинги по фишингу устарели. Новизна подхода –включение в программу киберучений синтезированного звонка. Сотруднику звонит «робот-руководитель» с тестовым заданием. Анализ реакции (поверил/переспросил/повесил трубку) – самый эффективный способ выработать рефлекс.

В связи с этим создание дипфейка ради получения выгоды не считалось преступлением, пока не наступали последствия в виде кражи денег (мошенничество). 27 января 2026 г. депутаты от партии «Справедливая Россия» внесли за рассмотрение Госдумы поправки в Уголовный кодекс для статьи 272.1, который вводит ответственность за саму несанкционированную обработку биометрических данных с целью синтеза изображения или голоса гражданина[227].

Законопроект дополнит часть 1 статьи 272.1 УК РФ таким самостоятельным действием, как «автоматизированная обработка». Изменение позволит квалифицировать как преступление факт незаконной автоматизированной обработки персональных данных, полученных неправомерным путём, независимо от последующих действий с ними[228].

Параллельно с техническими методами защиты формируется и правовой контур противодействия. Федеральный закон от 30.11.2024 № 421-ФЗ ужесточил ответственность за незаконную автоматизированную обработку персональных данных, а законопроект о внесении изменений в ст. 272.1 УК РФ (внесён депутатами от «Справедливой России» 27 января 2026 г.) вводит в качестве образующего признака сам факт несанкционированной обработки биометрии для синтеза изображения или голоса. Из этого следует, что уголовно наказуемы становятся не только последствия но и сам факт создания цифрового клона человека без его согласия, что выступает сильной превентивной мерой против создания цифрового клона человека.

Подводя итог, следует вывод, что в условия развития deepfake в сочетании с социальной инженерией, человеческий фактор из слабого звена превратился для злоумышленников в основополагающий вектор атак, способный обойти даже MFA, традиционно основанные на знании, владении и биометрии. В ответ на это же требуется адаптировать системы защиты под новые виды угроз. Только сочетание технологической бдительности, введённой в привычку сотрудникам, и актуального законодательства позволит создать эффективную систему против новых угроз.

---

[225] Об информации, информационных технологиях и о защите информации : Федеральный закон от 27 июля 2006 г. № 149-ФЗ (ред. от 09.03.2021) // СЗ РФ. 2006. № 31 (1 ч.). Ст. 3448; Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи» // СЗ РФ. 2003. № 28. Ст. 2895; Федеральный закон «О техническом регулировании» от 27 декабря 2002 г. № 184-ФЗ // СЗ РФ. 2002. № 52. Ст. 5140; и др.

[226] ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью // Электронный фонд правовых и нормативно-технических документов. URL: https://docs.cntd.ru/document/1200044724 (дата обращения: 20.0.2026); ГОСТ Р 52448-2005 Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения // ФСТЭК России. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/113-gosudarstvennye-standarty/377 (дата обращения: 20.0.2026); Национальный стандарт Российской Федерации Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Часть 3. Анализ методов доверия. ГОСТ Р 54583-2011/ ISO/IEC/TR 15443-3:2007 // Электронный фонд правовых и нормативно-технических документов. URL: https://docs.cntd.ru/document/1200095101 (дата обращения: 20.0.2026); и др.

[227] Обзор изменений в законодательстве за январь 2026 года // Zlonov Hub. URL: https://hub.zlonov.ru/laws/reviews/2026-01-USSC-review (дата обращения: 10.05.2026).

[228] О внесении изменений в Уголовный кодекс Российской Федерации : Федеральный закон от 30.11.2024 № 421-ФЗ. URL: https://www.consultant.ru/law/hotdocs/87301.html (дата обращения: 10.05.2026).

УДК 34:004.056(045)

И. Р. Юсупов,
обучающийся 3 курса Нефтекамского филиала
ФГБОУ ВО «Уфимский университет науки и технологий».
Научный руководитель: А. Р. Аюпова, канд. физ.-мат. наук, доцент
Нефтекамского филиала ФГБОУ ВО «Уфимский университет науки и технологий»,
г. Нефтекамск

Цифровой след при работе с электронными устройствами: проблемы организационно-правового обеспечения

Каждый раз, когда человек работает с электронным устройством, он оставляет за собой цепочку данных – цифровой след. Для криминалистики это ценнейший источник информации: именно по нему восстанавливают хронологию преступления, устанавливают личность злоумышленника, доказывают факт доступа к системе. Однако значение цифрового следа растёт вместе с числом преступлений, для раскрытия которых он необходим. По данным МВД России, в 2024 г. с использованием информационных технологий было совершено 765,4 тыс. преступлений – 40 % от всех зарегистрированных в стране. Совокупный ущерб превысил 200 млрд рублей, а раскрыто из них лишь 23 %[229]. В 2025 г. цифра несколько снизилась – до 675 тыс., однако доля в общей преступности осталась на уровне 38 %[230]. Один из главных ответов на вопрос «почему так мало раскрывают» – в том, что правовой и организационный механизм работы с цифровым следом серьёзно отстаёт от реальности. Именно эту проблему рассматривает данная статья.

Цифровой след – это совокупность данных, которые фиксируются при взаимодействии пользователя с устройствами и сетями. Часть из них человек оставляет осознанно: публикации в социальных сетях, сообщения, заполненные формы. Это активный след. Другая часть возникает без его ведома: IP-адреса, метаданные файлов, записи в системных журналах, история подключений – пассивный след[231]. В криминалистике важно различать понятия «цифровой след» и «виртуальный след». Виртуальный след – это изменение состояния информационной системы, например факт соединения или удалённый файл. Сам по себе он ещё не является доказательством: чтобы использоваться в суде, он должен быть зафиксирован на материальном носителе – скриншотом, образом диска, протоколом осмотра. Только тогда он становится частью цифрового следа в процессуальном смысле[232]. Источники цифрового следа зависят от типа устройства. На персональном компьютере это реестр системы, журналы событий, кэш браузера; на смартфоне – геолокация, базы данных мессенджеров, EXIF-данные фотографий; на устройствах интернета вещей – журналы взаимодействий и данные облачной синхронизации[233]. Каждый из этих источников имеет свою специфику с точки зрения того, насколько быстро данные исчезают и насколько сложно их извлечь.

Казалось бы, правовая база для работы с цифровым следом в России существует. Конституция (ст. 23) защищает тайну переписки[234]. УПК регулирует изъятие электронных носителей и доступ к переписке (ст. 164, 183, 185)[235]. Закон о персональных данных № 152-ФЗ охватывает большую часть данных, из которых состоит цифровой след[236]. Статья 272 УК устанавливает ответственность за неправомерный доступ к компьютерной информации[237]. Но стоит приглядеться – и картина становится куда менее оптимистичной.

Первая и самая серьёзная проблема: в УПК РФ нет понятия «электронное доказательство» как самостоятельного вида вообще. Следователи вынуждены применять к цифровым данным нормы, написанные для изъятия папок с бумагами. Это порождает ошибки при фиксации и регулярное оспаривание

---

[229] Краткая характеристика состояния преступности в Российской Федерации за январь–декабрь 2024 года // МВД России : [офиц. сайт]. URL: https://мвд.рф/reports/item/60248328/ (дата обращения: 12.04.2026).

[230] Краткая характеристика состояния преступности в Российской Федерации за январь–декабрь 2025 года // МВД России : [офиц. сайт]. URL: https://мвд.рф/reports/item/77848182/ (дата обращения: 12.04.2026).

[231] Вехов В. Б. О понятии и содержании электронно-цифрового следа // Вестник криминалистики. 2016. № 4. С. 11–17.

[232] Ищенко Е. П. Криминалистика : учебник для вузов. 6-е изд. М. : Юрайт, 2023. С. 312–315.

[233] Там же. С. 316–320.

[234] Конституция Российской Федерации (принята всенар. голосованием 12.12.1993, с изм., одобр. 01.07.2020) // СПС «КонсультантПлюс» (дата обращения: 13.04.2026).

[235] Уголовно-процессуальный кодекс Российской Федерации : Федеральный закон от 18.12.2001 № 174-ФЗ (действ. ред.) // СПС «КонсультантПлюс» (дата обращения: 13.04.2026).

[236] О персональных данных : Федеральный закон от 27.07.2006 № 152-ФЗ (действ. ред.) // СПС «КонсультантПлюс» (дата обращения: 13.04.2026).

[237] Уголовный кодекс Российской Федерации : Федеральный закон от 13.06.1996 № 63-ФЗ. Ст. 272 // СПС «КонсультантПлюс» (дата обращения: 13.04.2026).

допустимости доказательств в суде. Вторая проблема – скорость. Статья 185 УПК РФ требует судебного решения для доступа к электронным данным. Это разумная гарантия прав граждан, но она вступает в прямое противоречие с природой цифровых следов: оперативная память компьютера обнуляется при выключении, временные файлы перезаписываются через часы, а журналы многих систем работают по принципу циклической замены старых записей новыми. Пока идёт оформление судебного разрешения – доказательства исчезают. Это и есть тот самый «юридический вакуум», о котором пишут специалисты в области цифровой криминалистики. Третья проблема – в самом тексте закона. Примечание к ст. 272 УК РФ определяет компьютерную информацию как сведения в форме «электрических сигналов». Определение устарело: данные в блокчейне, QR-коды, журналы IoT-устройств под него не подпадают. А значит, защита таких данных от неправомерного доступа юридически неочевидна.

Для сравнения: в ЕС регламент GDPR предусматривает штрафы до 4 % от годового мирового оборота компании или 20 млн евро за нарушения в сфере персональных данных[238]. В России аналогичная санкция по ст. 13.11 КоАП РФ составляет до 6 млн рублей – при повторном нарушении до 18 млн рублей. Разрыв колоссальный, и он напрямую влияет на то, насколько серьёзно операторы относятся к защите данных. Отдельная проблема – трансграничные расследования. Россия не присоединилась к Будапештской конвенции о киберпреступности, однако в октябре 2025 г. подписала новую Конвенцию ООН против киберпреступности («Ханойскую»), разработанную по российской инициативе[239]. Это шаг в правильную сторону, но механизм реального взаимодействия с иностранными юрисдикциями при получении цифровых доказательств пока остаётся нерешённой задачей.

Предлагаемые изменения лучше начинать с процессуального уровня. В УПК РФ следует не просто упомянуть «электронное доказательство», а закрепить минимальные требования к работе с ним: как создаётся копия, чем подтверждается её неизменность, кто описывает исходный носитель и как сохраняется цепочка хранения. Тогда суд будет оценивать не абстрактный файл, а проверяемую последовательность действий, из которой видно, что данные не были изменены после изъятия. Для волатильных данных нужна отдельная срочная процедура: при риске утраты следователь фиксирует основания неотложности, копирует только необходимый объём информации и затем передаёт действия на судебный контроль. Такая модель сохраняет гарантии ст. 185 УПК РФ, но не делает их причиной исчезновения доказательств.

Следующий шаг касается материального права. Примечание к ст. 272 УК РФ стоит формулировать шире: компьютерная информация должна пониматься как данные независимо от способа хранения, обработки и передачи, а не только как «электрические сигналы». Тогда под правовую охрану без лишних споров попадут и облачные журналы, и записи IoT-устройств, и сведения в распределённых реестрах. На организационном уровне необходим не формальный центр «для отчётности», а постоянно действующая методическая площадка: типовые протоколы, обучение экспертов, консультации для регионов и единые требования к цифровым экспертизам. Международное сотрудничество после подписания Ханойской конвенции[240] тоже нужно переводить в практическую плоскость – с понятными каналами запроса, сроками ответа и правилами передачи копий цифровых доказательств.

Наконец, стоит подумать о том, как не допускать проблем, а не только реагировать на них. Принцип приватности по дизайну (privacy by design) – подход, при котором защита данных встраивается в систему на этапе её разработки, а не добавляется потом – уже закреплён в европейском законодательстве как обязательное требование. В России он пока остаётся добровольной практикой. Его законодательное закрепление снизило бы как число утечек, так и объём работы следствия: меньше утечек – меньше случаев, когда цифровой след оказывается в чужих руках.

Цифровой след сегодня – это главное доказательство по большинству уголовных дел, связанных с использованием технологий. Но правовая система, призванная это доказательство защищать и использовать, пока не поспевает за темпом изменений. Уголовно-процессуальный кодекс не знает электронных доказательств. Уголовный кодекс описывает компьютерную информацию языком, устаревшим два десятилетия назад. Организационные структуры не имеют ни единых стандартов, ни достаточных компетенций. Именно поэтому раскрываемость киберпреступлений составляет 23 % – а не потому, что следы не остаются. Они остаются. Просто мы пока не умеем с ними работать так, как того требует ситуация.

---

[238] General Data Protection Regulation (GDPR) 2016/679. URL: https://eur-lex.europa.eu/ (дата обращения: 13.04.2026); Кодекс Российской Федерации об административных правонарушениях : Федеральный закон от 30.12.2001 № 195-ФЗ (в ред. от 30.11.2024 № 420-ФЗ). Ст. 13.11 // СПС «КонсультантПлюс» (дата обращения: 14.04.2026).

[239] Конвенция Организации Объединённых Наций против киберпреступности: принята резолюцией ГА ООН 79/243 от 24.12.2024. URL: https://www.un.org/ru/documents/treaty/A-RES-79-243 (дата обращения: 14.04.2026).

[240] Там же.

Содержание

ОПИСАНИЕ ФУНКЦИОНАЛЬНОСТИ ИЗДАНИЯ:

Интерфейс электронного издания (в формате pdf) можно условно разделить на 2 части.

Левая навигационная часть (закладки) включает в себя содержание книги с возможностью перехода к тексту соответствующей главы по левому щелчку компьютерной мыши.

Центральная часть отображает содержание текущего раздела. В тексте могут использоваться ссылки, позволяющие более подробно раскрыть содержание некоторых понятий.

МИНИМАЛЬНЫЕ СИСТЕМНЫЕ ТРЕБОВАНИЯ:

Celeron 1600 Mhz; 128 Мб RAM; Windows XP/7/8 и выше; 8x DVD-ROM; разрешение экрана 1024×768 или выше; программа для просмотра pdf.

СВЕДЕНИЯ О ЛИЦАХ, ОСУЩЕСТВЛЯВШИХ ТЕХНИЧЕСКУЮ ОБРАБОТКУ И ПОДГОТОВКУ МАТЕРИАЛОВ:

Оформление электронного издания : Издательский центр «Удмуртский университет».

Макет и компьютерная верстка: И. А. Бусоргина.

Авторская редакция.

Подписано к использованию 11.08.2026
Объем электронного издания 3 Мб, тираж 10 экз.
Издательский центр «Удмуртский университет»
426034, г. Ижевск, ул. Ломоносова, д. 4Б, каб. 021
Тел.: +7(3412)263-751 E-mail: editorial@udsu.ru